UNIVERSIDADE FEDERAL DO PARANÁ

LIGIA ELIANA SETENARESKI

FISCALIZAÇÃO DA NEUTRALIDADE DA REDE E SEU IMPACTO NA EVOLUÇÃO DA INTERNET

CURITIBA

2017

LIGIA ELIANA SETENARESKI

FISCALIZAÇÃO DA NEUTRALIDADE DA REDE E SEU IMPACTO NA EVOLUÇÃO DA INTERNET

Tese apresentada como requisito parcial à obtenção do grau de Doutor em Ciência da Computação, no Programa de Pós-Graduação em Informática, do Setor de Ciências Exatas, da Universidade Federal do Paraná.

Orientador: Prof. Dr. Elias P. Duarte Jr.
Coorientadora: Prof. Dr. Leticia Mara Peres

CURITIBA

2017

S495 Setenareski, Ligia Eliana
Fiscalização da neutralidade da rede e seu impacto na evolução da internet / Ligia Eliana Setenareski. – Curitiba, 2017.
202 f. : il., grafs.

Orientador: Prof. Dr. Elias P. Duarte Jr.
Co-orientadora : Prof. Dr. Leticia Mara Peres
Tese (doutorado) – Universidade Federal do Paraná, Setor de Ciências Exatas, Programa de Pós-Graduação em Informática.
Inclui referências

1. Internet. 2. Neutralidade da rede. I. Duarte Junior, Elias Procopio. II. Peres, Leticia Mara. III. Universidade Federal do Paraná. Setor de Ciências Exatas. Programa de Pós-Graduação em Informática. IV. Título.

CDD 004.678

Andrea Carolina Grohs CRB 9/1.384

MINISTÉRIO DA EDUCAÇÃO
SETOR CIÊNCIAS EXATAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO INFORMÁTICA

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação em INFORMÁTICA da Universidade Federal do Paraná foram convocados para realizar a arguição da tese de Doutorado de **LIGIA ELIANA SETENARESKI** intitulada: **Fiscalização da Neutralidade da Rede e seu Impacto na Evolução da Internet**, após terem inquirido a aluna e realizado a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.
A outorga do título de doutor está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

Curitiba, 15 de Dezembro de 2017.

ELIAS PROCÓPIO DUARTE JUNIOR
Presidente da Banca Examinadora

LETICIA MARA PERES
Coorientador - Avaliador Interno

WALTER TADAHIRO SHIMA
Avaliador Externo

ROBERTO PEREIRA
Avaliador Interno

ANDRÉ RICARDO ABED GRÉGIO
Avaliador Interno

LISANDRO ZAMBENEDETTI GRANVILLE
Avaliador Externo

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Coordenação de Pós-Graduação em Informática

DEDICATÓRIA

Ao amor da minha vida,

Marcos Sfair Sunyê.

Porque, como dizia a minha amada mãe: **como é bom amar alguém!**

AGRADECIMENTO

Agradeço ao Prof. Dr. Elias P. Duarte Jr. pela paciência, pela disponibilidade, pela sua maravilhosa capacidade em ouvir. Por me conduzir, me fazer enxergar e entender o que eu precisava em cada momento para seguir em frente. Você foi fundamental para eu chegar até aqui!

Agradeço à Prof. Drª. Leticia Mara Peres pela confiança que depositou em mim, ao me aceitar inicialmente como sua orientada. Por acreditar que eu daria conta. Teu apoio foi fundamental quando eu mais precisei!

Agradeço ao Prof. Dr. Luis Carlos Erpen de Bona pela paciência em ensinar repetidas vezes até eu conseguir caminhar sem medo pela imensidão de textos, sobre ferramentas computacionais da área de redes, e me sentir segura para trabalhar com eles.

Agradeço ao Lucas Henrique Gonçalves, meu parceiro de jornada no mesmo tema, ele em seu mestrado e eu no meu doutorado. Parceria forte, gratificante e imprescindível para evitarmos a duplicação de trabalho e alcançarmos nossos objetivos.

Agradeço ao Thiago Garrett parceiro de jornada no doutorado de mesmo tema e na elaboração do *survey*. Seu conhecimento técnico foi imprescindível para alcançarmos nosso objetivo.

Agradeço ao Maycon Johnes Cortez e ao Edno Mendes de Lima Júnior pela tradução do resumo para a língua inglesa, que foi impecável.

Agradeço à Paula Carina de Araújo pelo primeiro levantamento bibliográfico relativo à coleta das definições sobre o tema.

Agradeço ao João Batista Masicz pelo atendimento rápido e infalível em sua copiadora, ao fazer as inúmeras cópias, das inúmeras versões de cada capítulo, e de tudo o mais que precisei.

Agradeço à Claudia Regina Camargo e a Alessandra Belézia Araujo pela ajuda com as tecnologias e com as minhas apresentações, ouvindo e marcando o tempo.

Agradeço ao Guilherme Luiz Cintra Neves pela ajuda no site do observatório, que criei como um dos resultados desta tese, à Joice Cardoso Banczynski pela logomarca do observatório, e à Caroline da Rocha Franco, pela primeira revisão do meu capítulo sobre a regulação. E, agradeço a vocês e aos demais membros do Comitê Gestor do Observatório da Neutralidade da Rede, por aceitarem o convite de enfrentar este desafio. Por acreditarem junto comigo que poderia valer a pena!

Agradeço à Andrea Carolina Grohs pela ficha catalográfica desta tese que fez prontamente!

Agradeço aos meus irmãos: Glicínia Eliza Setenareski Piasecki; Pedro Setenareski Filho; Ana Maria Setenareski Ahrens; Lia Mara Setenareski Magrin; Ana Néri Setenareski Lopes, Lília Márcia Setenareski e Moisés Vinicius Setenareski, pelo amor e compreensão à minha ausência durante este longo período de estudo.

À proteção espiritual que sinto existir e que me faz acreditar em mim e seguir em frente.

RESUMO

Desde 2002 temos presenciado um longo e controverso debate mundial sobre a Neutralidade da Rede, tema que envolve aspectos políticos, legais, econômicos, sociais, éticos, técnicos e de competitividade e inovação. A diversidade de aspectos considerados em torno deste tema leva a pontos de convergência e de divergência de opiniões, de acordo com os interesses dos agentes envolvidos. A Neutralidade da Rede refere-se à Internet aberta, na qual os usuários podem transitar de acordo com a sua liberdade de escolha. Em linhas gerais, a Neutralidade da Rede significa que os provedores de Internet, denominados ISPs (*Internet Service Providers*) não podem bloquear, estrangular, ou priorizar o conteúdo que trafega em suas redes. E, ainda, a Neutralidade da Rede significa que o ISP só pode cobrar do usuário final uma única vez pelo acesso à sua rede, e não pode cobrar dos provedores de conteúdo pelo conteúdo que trafega na sua rede. Nesta mesma senda, encontra-se o problema da violação ou da quebra da Neutralidade da Rede. Em traços largos, pode-se afirmar que ao longo deste tempo em que perdura o debate, os ISPs têm apresentado as mais diversas formas de violar a Neutralidade da Rede. Estas violações são detectadas e relatadas por usuários finais, ou por organizações, ou por membros da comunidade técnico-científica. Esta comunidade tem criado e utilizado mecanismos computacionais para monitorar o tráfego da Internet. Estes mecanismos computacionais têm por finalidade detectar alguma violação ou inconformidade com os preceitos da Neutralidade da Rede. Dentre as violações efetuadas pelos ISPs encontram-se os bloqueios de acesso a conteúdos, aplicações e portas; o estrangulamento e a diferenciação de tráfego; a velocidade ofertada abaixo da velocidade mínima contratada; a degradação do desempenho da rede; a oferta do serviço chamado de taxa zero, que discrimina e prioriza o tráfego; além de outras. Os ISPs, notadamente opositores à Neutralidade da Rede, continuam exercendo pressão junto às agências reguladoras e junto a políticos, a fim de impedir, retardar ou, até mesmo, modificar normatizações já instituídas. Isto comprova a permanência do debate, sem qualquer demonstração de previsão temporal em curto prazo para solucioná-lo. Como resultado de pesquisa, esta tese contribui para os avanços na área com a descrição de esforços mundiais de normatização bem como com o relato de diversos estudos de caso de violações nos cinco continentes. Esta tese também descreve ferramentas e estratégias desenvolvidas para detectar algum tipo de violação à Neutralidade da Rede. Além disso, é apresentado um estudo preliminar sobre uma possível correlação entre a regulação da Neutralidade da Rede e a evolução da infraestrutura da Internet no mundo. E, ainda, com o objetivo de contribuir de forma específica com o avanço deste tema no Brasil, apresenta um panorama dos agentes envolvidos neste contexto e o papel de cada um. E, finalmente, foi criado o Observatório da Neutralidade da Rede como uma ferramenta de controle social, para todos os aspectos inerentes à Neutralidade da Rede, a ser utilizada pela sociedade brasileira.

Palavras-chave: Detecção de Violação à Neutralidade da Rede; Regulação da Neutralidade da Rede; Observatório de Neutralidade da Rede; Ferramentas computacionais para a Neutralidade da Rede.

ABSTRACT

Since 2002 we have witnessed a long and controversial debate around Net Neutrality, a subject that encompasses multiple aspects, not only technical but also political, legal, economic, social, ethical, and also those related to competitiveness and innovation. The diversity of aspects around this subject raises opinions that both converge and diverge, according to the interests of the parts involved. Net Neutrality refers to an Open Internet that does not restrict users, enforcing their free choice. According to Net Neutrality principles, Internet Service Providers (ISP) cannot block, throttle or create fast tracks for any kind of pick traffic on their network. Furthermore, Net Neutrality means that an ISP is only allowed to charge end users once for the access to its network, and cannot charge content providers for making their content available. The Net Neutrality debate involves not only what is required/wanted but also the issue of Net Neutrality violations. It is possible to say that since the debate has started, ISPs have been shown to violate multiple Net Neutrality principles. Violations have been detected and reported by end users, or by organizations or by the technical community. This community has also devised strategies to monitor Internet traffic with the purpose of detecting violations or any type of non-compliance with the basic Net Neutrality principles. The ISP violations that have been reported include: blocking access to specific content, applications or ports; throttling and traffic discrimination; offering a network speed that is lower than the minimum speed agreed with the user; delivering low network performance; offering zero-rate services which discriminate and prioritize the traffic; among many others. ISPs, notably Net Neutrality opponents, continue to exert pressure on regulators and politicians to prevent, delay or even modify existing regulations. This proves that the debate has continued, without any hint that it will be solved in the short term. One of the contributions of this thesis is a comprehensive description of global regulatory efforts including several case studies of Net Neutrality violations that have occurred across the five continents. This thesis also presents a comprehensive survey of tools and strategies developed to detect Net Neutrality violations. In addition, a preliminary study is presented on a possible correlation between the establishment of Net Neutrality regulations and the evolution of the Internet infrastructure worldwide. Another contribution that has the specific purpose of contributing to the advancement of this theme in Brazil is the description of the agents involved in enforcing Net Neutrality in the country. Finally, the Network Neutrality Observatory was created as a tool that can enable social control of all the aspects inherent to Network Neutrality in Brazil.

Keywords: Detection of Net Neutrality violations; Net Neutrality Regulations; Net Neutrality Observatory; Net Neutrality Tools.

PUBLICAÇÕES DERIVADAS DA TESE

FISCALIZAÇÃO DA NEUTRALIDADE DA REDE E SEU IMPACTO NA EVOLUÇÃO DA INTERNET

Publicação 1

Título: Fiscalização da Neutralidade da Rede: Conceitos e Técnicas.

Autores: Ligia E. Setenareski em co-autoria com:

Thiago Garrett, Letícia M. Peres, Luis C. E. Bona, Elias P. Duarte Jr.

Publicação: publicado como *Minicurso do XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos - SBRC 2017,* pp. 1-50.

Link: https://sbrc2017.ufpa.br/wp-content/uploads/2017/05/proceedingsMinicurso2017.pdf

Publicação 2

Título: Monitoring Network Neutrality: A Survey on Traffic Differentiation Detection.

Autores: Ligia E. Setenareski em co-autoria com:

Thiago Garrett, Leticia M. Peres, Luis C. E. Bona, Elias P. Duarte Jr.

Publicação: submetida para o periódico *IEEE Communications Surveys &* Tutorials, pp. 1-30.

Publicação 3

Título: Impactos da regulação da Neutralidade da Rede na evolução da infraestrutura da Internet: uma investigação preliminar da correlação.

Autores: Ligia E. Setenareski em co-autoria com:

Lucas H. Gonçalves; Walter Shima; Luis C. E. Bona; Letícia M. Peres; Elias P. Duarte Jr.

Publicação: submetida para a *Revista de Economia Política*, pp. 1-25.

Observatório da Neutralidade da Rede

Foi também construído e disponibilizado na web o Observatório da Neutralidade da Rede - https://observatorio.c3sl.ufpr.br/neutralidadedarede/.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

CAPÍTULO I

INTRODUÇÃO

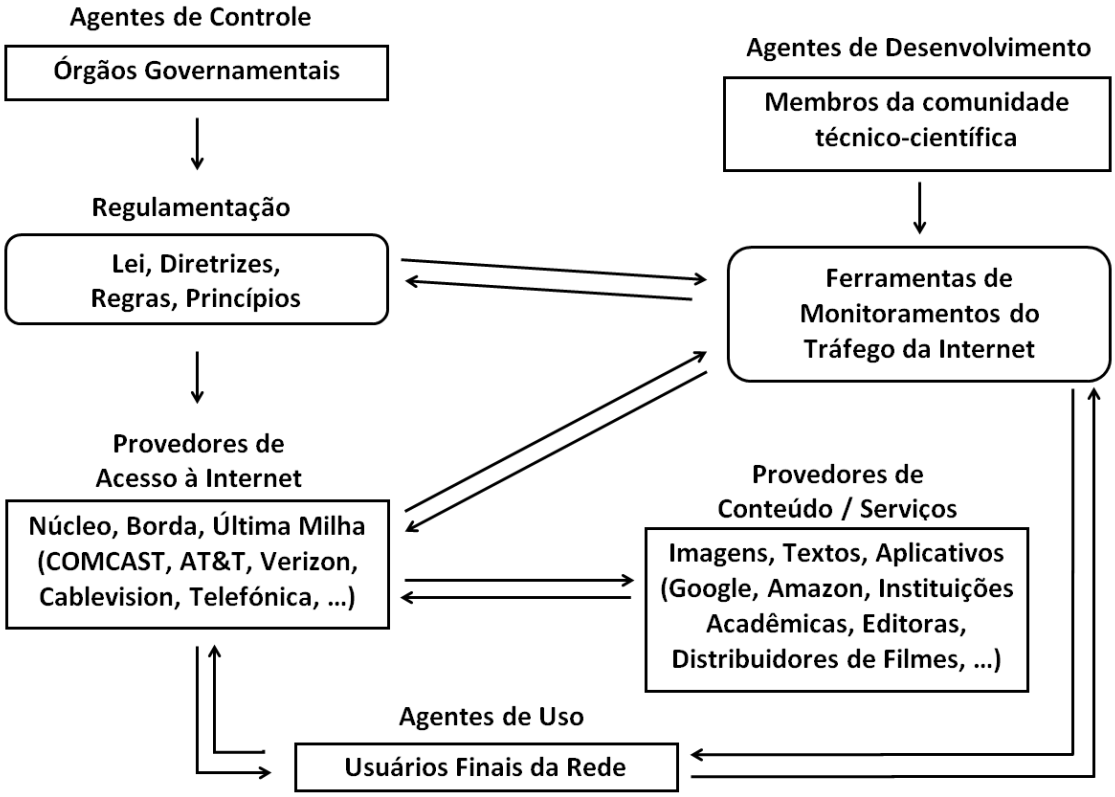
Desde 2002 temos presenciado um longo e controverso debate mundial sobre a Neutralidade da Rede, tema que envolve aspectos políticos, legais, econômicos, sociais, éticos, técnicos e de competitividade e inovação (WU, 2002; WU, 2003; YOO, 2005; HAHN; WALLSTEN, 2006; CROWCROFT, 2007; MARSDEN, 2008; VAN SCHEWICK; FARBER, 2009; BERNERS-LEE, 2010; BEREC, 2011; BEREC, 2012a; KRÄMER; WIEWIORRA; WEINHARDT, 2013; SCOTT, 2014; NET..., 2015a). A Neutralidade da Rede refere-se à Internet aberta, na qual os usuários podem transitar de acordo com a sua liberdade de escolha (BERNERS-LEE, 2010; FCC, 2015b; NET..., 2015a). Em linhas gerais, a Neutralidade da Rede significa que os provedores de serviços de acesso à Internet, denominados ISPs (*Internet Service Providers*) não podem bloquear, estrangular, ou criar pistas rápidas (priorização) para o conteúdo que trafega em suas redes (FCC, 2015b). E, ainda, a Neutralidade da Rede significa que o ISP só pode cobrar do usuário final uma única vez pelo acesso à sua rede, e não pode cobrar dos provedores de conteúdo pelo conteúdo que trafega na sua rede (HAHN; WALLSTEN, 2006).

Nesta mesma senda, encontra-se o problema da violação ou da quebra da Neutralidade da Rede. Em traços largos, pode-se afirmar que ao longo deste tempo em que perdura o debate, os ISPs têm apresentado as mais diversas formas de violar a Neutralidade da Rede (TELUS..., 2005; TOPOLSKI, 2007; KENDRICK, 2009; LING et al., 2010; SFAKIANAKIS; ATHANASOPOULOS; IOANNIDIS, 2011; MUELLER; ASGHARI, 2012; WEBER et al., 2013; ESNAASHARI, 2014; RISLEY, 2015; CAMPBELL, 2016). Estas violações estão retratadas em estudos de caso, em cartas, em artigos, ou ainda, em processos judiciais. Estas violações são detectadas e relatadas por usuários finais, ou por organizações, ou por membros da comunidade técnico-científica. A comunidade tem criado e utilizado mecanismos computacionais para monitorar o tráfego da Internet. Estes mecanismos computacionais têm por finalidade detectar alguma violação ou inconformidade com os preceitos da Neutralidade da Rede. Dentre

as violações efetuadas pelos ISPs encontram-se: os bloqueios de acesso a conteúdos, aplicações e portas; o estrangulamento e a diferenciação de tráfego; a velocidade ofertada abaixo da velocidade mínima contratada; a degradação do desempenho da rede; a oferta do serviço chamado de taxa zero (*zero rating)*; além de outras. Na prática da taxa zero, ao tornar o acesso ilimitado para alguns aplicativos e limitado para todos os outros na Internet, o ISP está, em termos técnicos, efetuando diferenciação, discriminação e priorização de tráfego.

O debate da Neutralidade da Rede envolve fundamentalmente cinco agentes, que se inter-relacionam conforme exposto na Figura 1: (i) os governos dos países que buscam elaborar Leis, definir políticas, ou estabelecer diretrizes e critérios para o trânsito na Internet de modo a mantê-la neutra; (ii) os provedores de serviços de acesso à Internet que, por sua vez, devem respeitar o que foi estabelecido para um trânsito considerado neutro, sem usar qualquer tipo de manipulação que venha a interferir em qualquer ponto do tráfego ou em seu conteúdo; (iii) os provedores de conteúdo que esperam ver transitar aquilo que disponibilizam ao usuário final da rede, sem qualquer tipo de interferência que venha ferir os preceitos da Neutralidade da Rede, e sem que necessitem pagar mais por isto; (iv) os usuários finais que esperam receber o que buscam, sem que tenha havido qualquer interferência em qualquer ponto da rede, e que esperam receber dos ISPs os serviços ofertados de acordo com o que foi estipulado nos contratos firmados com eles, e (v) os membros da comunidade técnico-científica que, atentos ao debate, criam ferramentas, mecanismos, algoritmos e técnicas, que buscam garantir a detecção da efetividade da aplicação do que foi estabelecido nas normatizações para uma rede neutra, ou a detecção da sua violação de alguma forma.

FIGURA 1 - OS PRINCIPAIS AGENTES ENVOLVIDOS NO DEBATE DA NEUTRALIDADE DA REDE



Fonte: O autor (2017).

1.1. MOTIVAÇÃO

A controvérsia em torno da Neutralidade da Rede basicamente diz respeito às ações que são permitidas, e aquelas que são proibidas aos ISPs. Desde o início do debate permanece o conflito entre os interesses dos governos em regular ou normatizar como o tráfego da Internet deve ser gerido, *versus* os interesses das empresas, neste caso os ISPs que, em geral, argumentam que o mercado, neste sentido, deveria permanecer livre de regulação. Em meio a isto se encontra o usuário da Internet, que espera ter seu direito de livre trânsito respeitado. Desta forma, a essência do debate se resume no conflito entre os interesses públicos e privados.

Quando o órgão regulador americano, a FCC (*Federal Communications Commission*) (FCC, 2002) classificou o serviço doméstico de Internet de alta velocidade como "serviço de informação" em 2002, o fato gerou polêmica porque este serviço era considerado como um serviço básico, e os ISPs eram considerados provedores de bens comuns, como os provedores de telefonia. Assim, a partir do momento em que a FCC

fez a classificação do serviço de acesso à Internet como “serviço de informação”, e não de “telecomunicação”, deu-se início ao debate sobre as questões que envolvem o trânsito na Internet e a sua regulação, debate este, denominado por Tim Wu, também em 2002, como Neutralidade da Rede (WU, 2002).

Em 2003, Tim Wu junta-se a Lawrence Lessig, um dos criadores da Creative Commons (LESSIG, 2001), para enviar uma carta à FCC na qual apresentam uma proposta de regime de Neutralidade da Rede. Esta carta foi projetada para encontrar um equilíbrio entre a proibição de operadores de banda larga em restringir as ações dos usuários, e a liberdade geral dada ao operador para gerenciar o consumo de largura de banda. Este regime adota o princípio básico de que operadores de banda larga devem ter total liberdade de policiar a si próprios, enquanto restrições devem ser vistas com desconfiança (WU; LESSIG, 2003). A partir daí, o debate em torno da Neutralidade da Rede foi se tornando persistente, angariando em sua defesa, além de muitos indivíduos ao redor do mundo, também importantes empresas provedoras de conteúdo como Google, Netflix e BitTorrent e, em sua oposição, principalmente os operadores de telecomunicações, como AT&T, Comcast, e Verizon.

Uma questão que se encontra no cerne do debate da Neutralidade da Rede diz respeito à manutenção da inovação em todas as camadas da rede, e não somente nos serviços ofertados por meio dela. Existe a preocupação relativa aos investimentos na expansão da infraestrutura física para suportar o tráfego de forma igualitária, ao mesmo tempo em que este se torna cada vez mais denso. Segundo Alan Joch, os defensores da Neutralidade da Rede procuram proteger os usuários de práticas de negócios potencialmente prejudiciais. Estes defensores argumentam que a legislação manterá os ISPs sob controle. Os defensores seguem o princípio que os usuários da Internet devem ser capazes de acessar qualquer conteúdo da Web ou usar quaisquer aplicativos, sem restrições ou limitações de seu provedor. Por outro lado, também segundo o autor, os céticos descartam a ideia de que a falta de controles adicionais para a Internet está colocando em risco a sociedade. Estes argumentam que o *status quo* gera um mercado competitivo (JOCH, 2009).

Como defensor da Neutralidade da Rede, Tim Wu ressalta que este ambiente competitivo da inovação centrada na Internet gera conflitos entre os interesses privados dos provedores de banda larga e os interesses públicos, fazendo com que os reguladores das comunicações precisem estar atentos (WU, 2003). Diante disso, o órgão regulador do Japão, o MIAC (*Ministry of Internal Affairs and Communications*), diz que há uma

necessidade crescente de formar consenso de ampla base sobre o desenvolvimento de políticas para uma concorrência leal e efetiva no mercado de banda larga. Isto é, salvaguardas são necessárias para eliminar restrições e obstáculos à concorrência na construção, operação e uso, incluindo a partilha de custos das redes como um todo, entre as muitas partes interessadas em cada camada (MIAC, 2007).

Se a inovação é tipicamente orientada para os usuários (MARSDEN, 2008), as implicações são que a inovação é incentivada pela interoperabilidade e pelo acesso aberto; em geral garantindo que o conteúdo possa ser compartilhado livremente entre esses usuários. Entretanto, Christopher Yoo, em oposição, argumenta que a adoção generalizada dos protocolos TCP/IP, dá à Internet uma interoperabilidade universal, gerando divergências entre os vários lados do debate da Neutralidade da Rede, inclusive levantando questionamento sobre quem pode estar bloqueando o acesso aos conteúdos e às aplicações (YOO, 2005). E, para o órgão regulador canadense, a CRTC (*Canadian Radio Television and Telecommunications Commission*), a questão é se esta inovação continuará a vir e, também, se os operadores de rede poderão suportar o tráfego gerado por esta inovação. Salienta que no Canadá a alta taxa de adoção dos serviços de Internet de banda larga, e a utilização de novos serviços inovadores pelos canadenses, levaram a um crescimento constante do tráfego na Internet (CRTC, 2009). Portanto, um problema real é saber se é chegado o momento de tomar as medidas concretas, técnicas, legislativas ou outras, para garantir que a Internet continue a funcionar como um meio aberto, e não discriminatório para a troca de ideias e para a inovação (WEITZNER, 2008).

Deste modo, pode-se dizer que o ponto nevrálgico do debate da Neutralidade da Rede refere-se à gestão razoável do tráfego *versus* a manutenção da competitividade e da inovação. A gestão razoável do tráfego, por parte dos ISPs, deve ser feita de forma a garantir que o usuário final da rede receba a QoS (*Quality of Service*) mínima estabelecida no SLA (*Service Level Agreement*) firmado com ele. A gestão razoável do tráfego determina que qualquer interferência, que precise ser feita em benefício de toda a rede e de seus usuários, deve ser divulgada de forma transparente. De acordo com o órgão regulador norueguês, o NPT (*Norwegian Post and Telecommunications Authority*), é importante destacar que a Internet aberta e não discriminatória não se atribui a tudo, como por exemplo, a distribuição ilegal de conteúdo com direitos autorais com a ajuda de compartilhamento de sistemas P2P (*peer-to-peer).* Isto permanece como um ato ilegal pelo usuário. Como também, a prática atual dos ISPs

para bloquear pornografia infantil não infringe a Neutralidade da Rede. E o mesmo pode ser dito em relação a filtros de *spam* e medidas para contrariar ataques de negação de serviço e PCs infectados. Isto é feito no interesse de todos os usuários para que o ISP possa proteger a rede por meio da qual seus usuários se comunicam. E destaca ainda que, há tipos de aplicação cuja qualidade de serviço pode exigir tratamento especial (os chamados serviços especializados), e os exemplos disso são a telefonia e o vídeo. Cabe aos ISPs publicar, bem como informar todos os usuários, de todas as medidas que representem interferências não esperadas. (NETWORK..., 2009).

Assim sendo, as práticas de gerenciamento do tráfego efetuadas pelos ISPs podem ser consideradas tanto razoáveis, quanto não razoáveis, sob o ponto de vista dos benefícios para a rede e seus usuários. Scott Jordan analisa quatro perguntas que, segundo ele, podem ser usadas para determinar se uma prática de gerenciamento do tráfego é razoável ou não razoável: (i) Onde na rede, e em que camada, as técnicas de gerenciamento de tráfego são aplicadas? (ii) Que tipo de funcionalidade de gerenciamento de tráfego é aplicada? (iii) Quem decide se a prática de gerenciamento de tráfego é aplicada? e (iv) Com base em quê se decidiu aplicar a prática de gerenciamento de tráfego? (JORDAN, 2009a). O autor classifica as técnicas como não razoáveis se elas forem excessivamente anticompetitivas, causarem danos indevidos aos consumidores, ou prejudicarem injustificadamente a liberdade de expressão (JORDAN, 2009b).

De acordo com Marcel Dischinger e outros autores, muitos ISPs querem restringir que determinadas aplicações tenham requisitos de largura de banda que possam interferir descontroladamente na rede. Alguns também querem controlar aplicações como VoIP que reduzem a capacidade dos ISPs de lucrar com seus serviços, pois são aplicações competidoras. Em contraste, muitos provedores de conteúdo são contra a diferenciação de tráfego, porque dá aos ISPs o controle arbitrário sobre a qualidade do serviço experimentado pelos usuários (DISCHINGER et al., 2010). Para o provedor de rede, bloquear ou degradar aplicações selecionadas é uma solução rápida, que requer menos investimento do que a atualização da rede ou do que conceber uma solução de gerenciamento não discriminatória. Em um mundo sem regras de Neutralidade da Rede, os ISPs determinam quais aplicativos e conteúdo podem se tornar bem sucedidos, distorcendo a concorrência nos mercados de aplicações e conteúdos (VAN SCHEWICK; FARBER, 2009).

O BEREC (*Body of European Regulators for Electronic Communications*), associação dos órgãos reguladores da União Europeia, ressalta que o gerenciamento de tráfego é vital, devendo levar em conta os diferentes tipos de usuários, tecnologias de redes, e até mesmo os diferentes tipos de ofertas de acesso à Internet, incluindo os serviços especializados, como por exemplo, transmissão de vídeo. Para o BEREC, também é importante distinguir entre medidas de gerenciamento de tráfego problemáticas (consideradas não razoáveis) e não problemáticas (consideradas razoáveis), dependendo dos efeitos que estas medidas têm sobre o usuário final (BEREC, 2011). Em concordância, Frode Sørensen, conselheiro sênior do órgão regulador norueguês, afirma que é essencial que os serviços especializados não tenham um impacto negativo no tráfego da Internet, porque caso contrário, este seria efetivamente um furo na base da Neutralidade da Rede. Para ele, foi estabelecido um consenso que a Neutralidade da Rede aplica-se à Internet, e não a outras formas de redes de comunicações eletrônicas e, neste contexto, os chamados serviços especializados não são serviços de acesso à Internet (SØRENSEN, [2014a]).

A FCC esclarece que os serviços especializados se incluem nas exceções às suas regras da Internet aberta. Para a FCC, alguns serviços de dados, como determinadas ofertas de VoIP, monitores de saúde, ou sensores de consumo de energia, entre outros, podem ser oferecidos por um provedor de banda larga, mas comumente não fornecem acesso ao serviço de Internet. Deste modo, a FCC destaca que o termo “serviços especializados” pode ser confuso porque o ponto crítico não é se os serviços são "especializados", e sim que eles não são serviços de acesso à Internet de banda larga propriamente dita. Eles são serviços IP que não trafegam através do serviço de acesso à Internet em banda larga, como os serviços de VoIP, utilizados por muitos clientes de cabo e, portanto, não estão abrangidos pelas regras da Internet aberta. As regras da Internet aberta protegem o acesso ou o uso do serviço de acesso à Internet de banda larga em si. No entanto, se estes outros serviços forem fornecidos de uma forma que prejudique a finalidade das regras da Internet aberta, a Comissão reserva expressamente a sua autoridade de intervir. Por exemplo, isso ocorre quando um serviço é equivalente funcionalmente a outro serviço da Internet propriamente dita. A FCC vela explicitamente por este tipo de abuso e as suas ações são facilitadas pela exigência de transparência aos ISPs, em matéria de divulgação dos serviços que oferecem (FCC, 2015b).

Seguindo esta linha, o BEREC sustenta que os usuários finais precisam estar plenamente conscientes dos termos efetivos dos serviços oferecidos. Para isto, precisam de meios ou ferramentas adequadas para monitorar os serviços de acesso à Internet, permitindo-lhes conhecer a qualidade efetiva do serviço obtido, e também para detectar possíveis degradações. O BEREC identificou duas categorias principais de degradação de serviço: (i) o serviço de acesso à Internet considerado como um todo. A qualidade do serviço de acesso à Internet pode tipicamente ser comparada com os serviços especializados, e a questão é verificar se os serviços especializados foram priorizados em detrimento dos serviços de acesso à Internet; e (ii) a qualidade de serviço dos aplicativos individualmente. Nesta categoria encontram-se os casos de diferenciação de tráfego de aplicações específicas, tais como bloqueio VoIP, estrangulamento P2P e priorização de tráfego de conteúdo e aplicações específicas de provedores (BEREC, 2012a). Neste sentido, a FCC continua a exigir a divulgação de velocidade e latência real da rede, e também a exigir a divulgação da taxa de perda de pacotes. Entretanto, declinou em exigir a divulgação de corrupção de pacotes e do *jitter*, observando preocupações quanto à dificuldade de definir métricas adequadas (FCC, 2015c).

Notadamente, a gestão razoável do tráfego da rede implica em não haver prejuízo algum para a própria rede ou para qualquer usuário dela. Entretanto, a normatização do tráfego por si só não garante a sua aplicação de forma adequada por parte dos ISPs. É preciso que haja mecanismos efetivos de detecção da conformidade na aplicação dos princípios, das Leis, das regras, ou das normas estabelecidas.

1.2. QUESTÕES DE PESQUISA

Diante deste contexto complexo, sobre as questões que envolvem a Neutralidade da Rede e as limitações que envolvem a sua fiscalização para uma efetiva aplicação, esta tese apresenta as seguintes Questões de Pesquisa (QP).

QP I. Existem mecanismos computacionais, capazes de monitorar o tráfego da rede e detectar algum tipo de violação à Neutralidade da Rede? Quais são eles?

QP II. A regulação da Neutralidade da Rede contribuiu para a evolução da Internet?

QP III. Existe no Brasil algum observatório que permita à sociedade acompanhar as questões relacionadas à Neutralidade da Rede, tais como o

comportamento dos ISPs, quanto ao gerenciamento do tráfego efetuado em suas redes, e o comportamento da agência reguladora, quanto à fiscalização e possíveis punições aos ISPs, em caso de alguma violação à Neutralidade da Rede?

O desenvolvimento metodológico empregado nesta tese, com o intuito de encontrar as respostas às questões aqui levantadas, compreendeu seis momentos conforme segue. Inicialmente, foi efetuado o aprofundamento teórico quanto aos conceitos da Neutralidade da Rede e, também, quanto às questões e os agentes envolvidos em seu debate. No segundo momento, foram levantadas as normatizações referentes à Neutralidade da Rede. Isto ocorreu, em especial, por meio de consulta aos órgãos reguladores das telecomunicações de cada país e por meio do acompanhamento da mídia. No terceiro momento, buscou-se levantar, de forma exaustiva, na literatura pertinente, os mecanismos computacionais de detecção de violações à Neutralidade da Rede. No quarto momento, buscou-se levantar, na literatura pertinente, no acompanhamento da mídia e nos sites dos órgãos reguladores das telecomunicações, os relatos de casos reais de violações à Neutralidade da Rede, de forma a trazer à tona um panorama que envolvesse países dos cinco continentes, e que fosse o mais diverso possível. No quinto momento, o foco da pesquisa se volta especificamente para o Brasil. Neste momento, efetuou-se o aprofundamento na busca aos agentes envolvidos no debate da Neutralidade da Rede neste país e o papel de cada um. Esta busca foi realizada basicamente por meio do acompanhamento da mídia e dos sites pertinentes. A partir dos resultados encontrados foi criado o Observatório da Neutralidade da Rede no Centro de Computação Científica e Software Livre, da Universidade Federal do Paraná. Por fim, buscou-se efetuar o levantamento dos dados quanto à evolução da infraestrutura da Internet, em termos mundiais e econômicos. Para tanto, foram utilizadas bases de dados específicas da área, relatadas no Capítulo 6 desta tese.

1.3. PRINCIPAIS CONTRIBUIÇÕES

Da forma como foi concebida, esta tese fornece, em termos globais, várias contribuições para o avanço do debate da Neutralidade da Rede, dado seu caráter multidisciplinar. Em termos específicos, esta tese lança no Brasil as bases necessárias para o desenvolvimento de mecanismos computacionais de detecção de violações, e as bases necessárias para o controle social da Neutralidade da Rede. A primeira

contribuição é arrolar os mecanismos computacionais para detecção de violação ou quebra da Neutralidade da Rede. Outra contribuição é mostrar em que contexto o debate da Neutralidade da Rede surgiu, e como se desenvolveu em todo o mundo, levando às normatizações necessárias para manter o tráfego na Internet sem interferências indesejáveis aos usuários. Contribui também, na medida em que apresenta não apenas as ferramentas computacionais de detecção de algum tipo de violação à Neutralidade da Rede, mas também leva em conta que elas só têm efetividade num ambiente normatizado, com regras de comportamento definidas para os ISPs. Contribui ainda, ao mostrar em que medida a infraestrutura da Internet evoluiu ao longo dos últimos quinze anos, e a relação com a normatização da Neutralidade da Rede. E, finalmente, contribui ao criar o Observatório da Neutralidade da Rede a fim de fornecer a infraestrutura necessária ao monitoramento do comportamento dos ISPs e da agência reguladora do Brasil quanto à fiscalização e a aplicação da Legislação relativa à Neutralidade da Rede.

Dito de outro modo, de forma concreta, o desenvolvimento da pesquisa para esta tese resultou nas seguintes contribuições.

1. Elaboração de *survey*, submetido para periódico internacional, que faz um apanhado profundo das estratégias existentes para detecção de violações à Neutralidade da Rede e múltiplos relatos de casos reais de violações à Neutralidade da Rede.

2. Construção do Observatório da Neutralidade da Rede (https://observatorio.c3sl.ufpr.br/neutralidadedarede/), com caráter multidisciplinar, que servirá como ferramenta de controle social da Neutralidade da Rede para a sociedade brasileira.

3. Elaboração de artigo, submetido para periódico nacional, que expõe uma análise preliminar da correlação entre os panoramas mundiais da normatização da Neutralidade da Rede e da evolução da infraestrutura da Internet. Destaca-se que este artigo resultou da pesquisa conjunta com mestrando do Programa de Pós-Gradução em Políticas Públicas, em tema relacionado à Neutralidade da Rede, com foco na economia, descrito no capítulo 6 desta tese.

1.4. ORGANIZAÇÃO DESTA TESE

A organização deste trabalho é a seguinte. Na Introdução, a ênfase está nos princípios e fatos que deram início ao debate da Neutralidade da Rede. Do mesmo

modo, este capítulo enfatiza os aspectos relevantes que fundamentaram as normatizações lançadas pelos órgãos reguladores e que, ao mesmo tempo, se constituem na motivação à elaboração desta tese. E, ainda, este capítulo apresenta as questões de pesquisa a serem respondidas ao final desta tese. No Capítulo 2 o destaque está na conceituação e nos estudos de caso. Neste capítulo são elencadas as principais definições dadas à Neutralidade da Rede e aos temas relacionados. Também neste capítulo é mostrada a origem dessas definições. E, ainda, o foco se volta para os estudos de caso que tratam de algum tipo de violação à Neutralidade da Rede, encontrados em diversas partes do mundo e denunciados por usuários finais da Internet, por organizações, ou pela mídia. No Capítulo 3 são sintetizadas as normatizações que se constituem em diretrizes, regras, normas, ou Leis estabelecidas por vários países, formando um panorama mundial sobre o assunto. No Capítulo 4, a ênfase é dada sob a ótica da Ciência da Computação, nas ferramentas desenvolvidas por pesquisadores desta área. Estas ferramentas permitem que os aspectos técnicos, relacionados à Neutralidade da Rede, possam ser verificados. Elas monitoram o gerenciamento do tráfego da Internet, realizado pelos ISPs, a fim de detectar se há manipulação indevida por parte deles. Desta forma, os pesquisadores e suas ferramentas apoiam os governos e usuários finais na fiscalização da efetividade da Neutralidade da Rede. Isto ocorre porque os resultados dos monitoramentos podem vir a embasar as sanções dadas aos ISPs pelos órgãos reguladores. No Capítulo 5 é apresentado o Panorama da Internet no Brasil e o Observatório da Neutralidade da Rede, com a devida justificativa para a sua criação e as características que o compõe. No Capítulo 6, a ênfase é dada sob a ótica da economia, no panorama mundial da evolução da infraestrutura da Internet. Neste capítulo é apresentada uma investigação preliminar da correlação entre este panorama mundial da evolução da infraestrutura da Internet e o panorama mundial da normatização da Neutralidade da Rede. Finalmente, no Capítulo 7 são apontadas algumas conclusões a este estudo, e são elencadas algumas sugestões de estudos futuros relacionados ao tema aqui tratado. Também neste capítulo, são respondidas as questões de pesquisa levantadas nesta tese.

CAPÍTULO II

DEFINIÇÕES BÁSICAS E ESTUDOS DE CASO

Este capítulo visa apresentar definições da Neutralidade da Rede, inclusive definindo observatório de Neutralidade da Rede, um dos focos do trabalho. Este capítulo visa também listar outros trabalhos relacionados à Neutralidade da Rede e apresentar estudos de caso relativos à quebra da Neutralidade da Rede. Para tanto, o capítulo é subdividido em quatro seções: 2.1. Definições Básicas: Neutralidade da Rede; 2.2. Definições Básicas: Observatórios de Rede; 2.3. Outros Trabalhos Relacionados à Neutralidade da Rede; 2.4. Estudos de Caso Sobre Violações à Neutralidade da Rede; e 2.5. Considerações Finais.

2.1. DEFINIÇÕES BÁSICAS: NEUTRALIDADE DA REDE

Os fundamentos que sustentam a defesa da Neutralidade da Rede remetem à criação da Web. De acordo com Tim Berners-Lee (BERNERS-LEE; FISCHETTI, 2000; BERNERS-LEE, 2010), a *Web* evoluiu para uma ferramenta poderosa e onipresente porque foi construída sobre princípios igualitários, tais como: universalidade, no sentido que não importa o hardware, o software, a conexão de rede ou a linguagem usada, e o tipo de informação que trafega. Além disso, outro princípio é o fato de ser baseada em padrões abertos; e nos direitos humanos eletrônicos, ou seja, é uma rede livre de interferência. Outros princípios ainda incluem a proteção à confidencialidade dos dados, e a liberdade de expressão. Do mesmo modo, o projeto arquitetônico da Internet foi orientado por dois princípios fundamentais: (i) as mensagens são fragmentadas em pacotes de dados que são roteados através da rede de forma autônoma (princípio *end-to-end*) e (ii) tão rápido quanto possível (princípio do melhor esforço) (COMER, 2015). Isto implica que os nós intermediários, os chamados roteadores, não diferenciem pacotes com base no seu conteúdo ou fonte.

Estes princípios fundamentais sempre foram e continuam sendo, no contexto do debate da Neutralidade da Rede, os elementos-chave do espírito da Internet aberta. Essencialmente, eles estabelecem que todos os pacotes de dados enviados pela rede sejam tratados com igualdade, e que nenhum nó intermediário possa exercer controle sobre a rede como um todo (KRÄMER; WIEWIORRA; WEINHARDT, 2013). E, neste sentido, o BEREC esclarece que, na Neutralidade da Rede, a comunicação na rede consiste em transferir o tráfego independentemente do conteúdo e aplicações. Isto significa que os dados recebidos da camada de aplicação devem ser encaminhados de forma neutra pela camada de rede (BEREC, 2012a).

Autores como R. Hahn e S. Wallsten, embora destaquem que a Neutralidade da Rede não tem uma definição precisa e amplamente aceita, afirmam que um ponto básico é o fato dos provedores de serviço de banda larga cobrarem apenas uma vez dos consumidores o acesso à Internet. Além disso, os provedores de serviço de banda larga não podem favorecer um provedor de conteúdo sobre o outro. E, ainda, os provedores de serviço não podem cobrar dos fornecedores de conteúdo pelo envio de informações através de suas linhas de banda larga aos usuários finais. Para estes autores, a Neutralidade da Rede significa que provedores de banda larga não devem cobrar nada dos provedores de conteúdo, e devem cobrar os usuários finais apenas em certas formas prescritas (HAHN; WALLSTEN, 2006).

A *Internet Society*, uma das responsáveis pela governança da Internet, entende que a Neutralidade da Rede preconiza que o trânsito na Internet deve ser livre. Isso significa que o usuário da rede deve estar no controle da navegação que faz *online*. Significa também que as empresas que fornecem serviços de Internet devem tratar todos os conteúdos lícitos da Internet de forma neutra, porque estes são os princípios base da Internet. E, significa ainda, que a Neutralidade da Rede tornou-se um termo amplo, porém ainda mal definido. Isto porque o termo engloba uma ampla gama de objetivos políticos, incluindo a liberdade de expressão, a escolha do usuário, e a discriminação. E o termo engloba também as questões de negócios, incluindo o gerenciamento de tráfego de rede, a precificação e os modelos de negócios em geral. Além de tudo isso, a transparência é fundamental (INTERNET SOCIETY, 2015a).

Para Tim Berners-Lee, a Neutralidade da Rede é um princípio segundo o qual todos devem ter igual acesso aos conteúdos disponíveis *online* (SCOTT, 2014). Em concordância, a FCC explica que uma Internet aberta significa que os consumidores podem ir para onde querem na rede, e quando querem. Para a FCC esta é, na verdade, a

definição de Neutralidade da Rede. Neste contexto, os inovadores podem desenvolver produtos e serviços sem pedir permissão. Significa que os consumidores irão exigir mais e melhor largura de banda. E significa que os provedores de banda larga não podem bloquear, estrangular ou criar as chamadas "pistas rápidas" especiais para determinados conteúdos (FCC, 2015b).

Paul Ganley e Ben Allgrove esclarecem que a Neutralidade da Rede é uma questão complexa que deve fundir o interesse público com considerações legais, práticas e comerciais (GANLEY; ALLGROVE, 2006), e Jon Crowcroft propõe uma meta-definição que visa separar os diversos componentes do problema da seguinte forma: (i) neutralidade da conectividade (*Connectivity Neutrality*). Define a conectividade universal ponta a ponta; (ii) neutralidade do desempenho (*Performance Neutrality*). Define regras para o desempenho esperado, de uma forma mensurável, compreensível e transparente; (iii) neutralidade do serviço (*Service Neutrality*). Define regras para a disponibilização de novos serviços; e (iv) neutralidade no cruzamento das camadas (*Cross Layer Neutrality*). Define como as combinações de serviços são construídas e como o consumidor escolhe entre eles (CROWCROFT, 2007).

Embora as várias definições encontradas tragam diferenças entre si, elas não são contraditórias, elas são complementares. O acesso aberto à Internet está intimamente ligado à Neutralidade da Rede. Envolve a polarização entre o dever dos ISPs de manter o trânsito neutro, e o direito dos provedores de conteúdo de não precisar pagar para que seu conteúdo trafegue de forma igualitária pela rede. Envolve ainda o direito do usuário final em ter acesso ao conteúdo de sua escolha, em uma Internet de trânsito livre e neutro. É notório que, no seu início, a Internet era assim: o trânsito era livre e neutro até que os ISPs começaram a interferir no gerenciamento do tráfego, efetuando algum tipo de diferenciação, discriminação ou degradação. Este comportamento provocou o desequilíbrio, o caos no ecossistema da Internet. E a situação atual da Internet permanece em desequilíbrio, com vários conflitos que refletem os vários interesses dos agentes envolvidos no ecossistema.

2.2. DEFINIÇÕES BÁSICAS: OBSERVATÓRIOS DE REDE

O objetivo desta seção é apresentar uma definição para *observatório de Neutralidade de Rede*. Não foi encontrada qualquer definição relativa ao tema. Assim,

na ausência de definição inerente, e para efeitos deste estudo, foi criada uma definição que busca aproximar a definição do termo geral às características do termo específico. São relatadas aqui também, as iniciativas localizadas no Brasil quanto à criação de observatório de Neutralidade de Rede.

De acordo com o Dicionário do Aurélio, uma das definições de observatório é: "instituição que se dedica à observação, acompanhamento ou divulgação de determinados fenômenos ou informação" e outra definição, em termos mais genéricos, é: "lugar de onde se observa" (DICIONÁRIO..., 2016). Para efeitos desta tese, e partindo das definições acima apresentadas, o Observatório da Neutralidade da Rede no Brasil se destina a acompanhar o comportamento dos provedores de acesso à Internet brasileira quanto ao gerenciamento de tráfego efetuado pelos provedores em suas redes. Ao mesmo tempo, o Observatório se destina a acompanhar o comportamento da agência reguladora das telecomunicações no Brasil, quanto ao monitoramento do gerenciamento de tráfego efetuado pelos provedores de acesso à Internet, e quanto aos procedimentos adotados, relativos a eventuais violações à Neutralidade da Rede, e em concordância ao disposto na Legislação pertinente.

Existem no Brasil dois observatórios relacionados ao tema proposto neste estudo: (i) Observatório da Internet no Brasil. Mantido pelo CGI.br (Comitê Gestor da Internet no Brasil), este observatório de acordo com seu *site*[1],"é um projeto do CGI.br que representa um esforço permanente e sistemático – a partir de um prisma multissetorial – de observação, análise e documentação de políticas públicas, legislações, técnicas, práticas e eventos a respeito da Internet no Brasil e no mundo, tendo como referência para o seu funcionamento questões correlatas aos Princípios para a Governança e Uso da Internet no Brasil" (OBSERVATÓRIO..., 2016a); e (ii) Observatório do Marco Civil da Internet (OMCI). Este observatório foi criado no início de 2015, alguns meses após a publicação da Lei n° 12.965, de 2014. De acordo com o seu *site*[2] "o OMCI tem objetivos acadêmicos, sem vínculos político-partidários, e o foco principal na evolução do tema diante das principais decisões judiciais nacionais, incluindo os rumos tomados pela Jurisprudência, sem, no entanto, comentar especificamente os casos concretos e/ou decisões relacionadas [...] por se tratar de uma lei considerada modelo na proteção e defesa da privacidade e da liberdade de expressão, bem como da neutralidade da rede, consolida-se conjunta e colaborativamente uma base

[1]http://observatoriodainternet.br

[2]http://omci.org.br

de dados ampla e diversificada em auxílio dos julgadores, pesquisadores, estudantes e demais interessados no tema" (OBSERVATÓRIO..., 2016b).

Diante do exposto, nota-se que nenhum destes observatórios tem como objetivo, o que está sendo proposto neste estudo. Estes observatórios encontrados visam observar o que ocorre em toda a Internet, ou observar alguns aspectos específicos como os desdobramentos do Marco Civil da Internet no Brasil. Nenhum deles se propõe a observar os aspectos decorrentes da Lei brasileira da Neutralidade da Rede, no que diz respeito ao comportamento dos agentes envolvidos, a fim de monitorar a efetividade da aplicação da Neutralidade da Rede no Brasil.

2.3. OUTROS TRABALHOS RELACIONADOS À NEUTRALIDADE DA REDE

Considerando a vasta literatura encontrada sobre o tema da Neutralidade da Rede, foram selecionados e são relatados aqui nesta seção somente os trabalhos considerados como *surveys.* Assim, nesta linha, buscou-se mostrar aqui os *surveys* publicados ao longo do tempo em que perdura o debate da Neutralidade da Rede, e que, de alguma forma, possam ter relação com a abordagem desta tese.

No trabalho de 2007 (DONNET; FRIEDMAN, 2007), os autores concentram-se nas medições da topologia da rede, isto é, na representação da interconexão entre pares diretamente conectados na rede. Discutem a topologia no nível do protocolo IP; apresentando a topologia em nível de roteadores; e de sistemas autônomos, incluindo PoPs (Pontos de Presença). Embora parte dessa informação possa ser adquirida a partir de medições passivas, os pesquisadores obtiveram de medições ativas grande parte da topologia e suas características.

Em seu trabalho de 2008 (DEEB; O'BRIEN; WEINER, 2008), "*A Survey on Network Neutrality*", os autores buscam explicar os conceitos que englobam a Neutralidade da Rede, os seus prós e contras, e as suas implicações para a indústria, o governo e as universidades. Destacam também que procuram manter uma abordagem neutra na construção do próprio artigo.

No trabalho de 2009 (CALLADO et al., 2009), sobre o gerenciamento de tráfego da Internet, os autores procuram explicar os principais problemas e técnicas conhecidos no campo de análise de tráfego IP. Fazem a caracterização do tráfego separando-o em categorias baseadas em pacotes e baseadas em fluxo, e detalham as vantagens e

problemas de cada abordagem. Comparam os métodos de identificação de tráfego, e descrevem as medições ativas *versus* as medições passivas, para monitoramento.

No trabalho de 2013(GOMES et al., 2013), os autores examinam os métodos, técnicas e aplicações existentes sobre o tema da classificação de tráfego P2P, fazendo uma extensa avaliação da literatura e fornecendo uma análise abrangente dos conceitos e das estratégias de monitoramento de rede. Descrevem as abordagens existentes para a classificação de tráfego, explicando o seu modo de funcionamento, e em que situações elas são mais valiosas, e quais são suas limitações. Também incluem uma introdução ao tema da medição de tráfego para fins de monitoramento de rede P2P.

No estudo de 2014 (HOFSTEDE, 2014), os autores fornecem um tutorial integrado sobre monitoramento de fluxo. Neste tutorial discutem todos os aspectos de um monitoramento de fluxo baseado em *NetFlow*, cobrindo o espectro completo desde a observação de pacotes, até a medição e exportação de fluxos, incluindo a coleta e análise de dados. Mostram como as abordagens anteriormente opostas de inspeção profunda de pacotes, DPI (*deep packet inspection*), e monitoramento de fluxo se uniram em novas abordagens de monitoramento. Descrevem a história dos protocolos de exportação de fluxo colocando o tema em um contexto mais amplo e comparando-o com outras tecnologias relacionadas. Apresentam uma visão geral da arquitetura de monitoramento de fluxo típico e os conceitos mais importantes.

No *survey* de Vaibhav Bajpai e Jürgen Schönwälder, de 2015 (BAJPAI; SCHÖNWÄLDER, 2015), os autores apresentam uma taxonomia das plataformas de medição da Internet. Classificam estas plataformas de medição de desempenho com base em sua implantação de caso de uso: medições de acesso fixo, medições de acesso móvel, entre outras. Descrevem as características dessas plataformas, tais como sua cobertura, escalabilidade, duração, implantação de métricas e ferramentas de medição, bem como sua arquitetura e impacto global, e relatam os esforços atuais de padronização para tornar as plataformas de medição de desempenho interoperáveis.

Giuseppe Aceto e Antonio Pescapé apresentam em 2015 (ACETO; PESCAPÉ, 2015) um *survey* sobre a detecção da censura na Internet, no qual descrevem e discutem as técnicas, arquiteturas, ferramentas e plataformas disponíveis para detecção de censura, propondo um esquema de caracterização para analisá-las e compará-las.

Também é de 2015, o *survey* sobre a medição de redes móveis no qual os autores examinam as abordagens atuais para medição de desempenho e diagnóstico, além de prototipagem de aplicativos de redes móveis. Comparam as ferramentas

disponíveis e as suas deficiências no que diz respeito às necessidades dos desenvolvedores, dos operadores de rede e dos órgãos reguladores, proporcionando uma visão abrangente dos esforços de medição de banda de redes móveis e da avaliação de desempenho de aplicativos móveis (GOEL et al., 2015).

Nenhum trabalho encontrado traz a abordagem como a que está sendo proposta nesta tese, visto que nenhum deles apresenta panoramas mundiais sobre a normatização da Neutralidade da Rede e sobre os estudos de caso que retratam as suas violações. Do mesmo modo, nenhum trabalho traz as ferramentas computacionais disponíveis para detecção de algum tipo de violação da Neutralidade da Rede. E, principalmente, nenhum deles aponta para a necessidade de criação de observatório que vise monitorar a efetividade da Neutralidade da Rede.

2.4. ESTUDOS DE CASO SOBRE VIOLAÇÕES À NEUTRALIDADE DA REDE

O objetivo desta seção é mostrar um panorama mundial sobre as violações da Neutralidade da Rede. As denúncias relativas às violações às regras estabelecidas para a Neutralidade da Rede proliferam ao longo dos anos pelo caráter mundial que o tema vai tomando, devido ao aumento do número de países que vai definindo a sua normatização. Ao mesmo passo, estas denúncias vão sendo replicadas nos diversos *sites* de notícias, e os usuários da Internet vão se tornando participantes ativos no debate. Por conseguinte, diante do grande volume de estudos de caso encontrados, adotou-se como critério de seleção a variedade dos casos, a diversidade dos países onde os casos ocorreram, e a diversidade de agentes envolvidos, a fim de obter um panorama global e diversificado. Os estudos de caso são listados aqui em ordem cronológica.

Em 21 de julho de 2005, membros do sindicato canadense dos trabalhadores de telecomunicações, a TWU (*Telecommunications Workers Union*), entraram em greve contra a Telus, operador de telecomunicações canadense. Em consequência, em 22 de julho daquele ano, a Telus bloqueou o acesso aos seus assinantes de Internet, para o *site* Vozes de Mudança (*Voices for Change*). Este *site* era dirigido por e para os membros da TWU. A Telus alegou que o seu contrato de serviço com os assinantes lhe permitia bloquear qualquer *site* (TELUS..., 2005; AUSTEN, 2005).

Desde setembro de 2005 o *site* do Vuze[3], um cliente de BitTorrent para Mac, Windows, Android, e a maioria das distribuições Linux, disponibiliza uma lista dos chamados *Bad* ISPs por terem causado problemas para os seus usuários (REVISION..., 2005). Esta lista contém os ISPs que causaram problemas para clientes de BitTorrent, jogos *online* e/ou outros clientes P2P, incluindo uma descrição do problema.

Em 24 de julho de 2007 a ferramenta *Web Tripwires*, que detecta modificações em páginas *web* como vistas por clientes, foi ao ar e, no dia seguinte, apareceu em diversos *sites* de notícias de tecnologia. Com isto, os autores puderam testar mais de 50.000 clientes a partir de um único servidor. A análise abrangeu os dados coletados durante 20 dias, englobando a maioria do tráfego recebido. Como resultado, 657 clientes relataram ao menos um tipo de modificação indevida ou inesperada. Cerca de 70% das modificações foram causadas por *proxies* do lado do cliente, tais como bloqueadores de *popup*, mas 46 endereços IP relataram mudanças que pareciam ser intencionalmente causadas por seu próprio ISP. Os autores também descobriram que os *proxies* utilizados em 125 clientes deixaram a página vulnerável a ataques (REIS et al, 2008).

Também em 2007, em um fórum de discussão da DSLREPORTS, Robb Topolski (TOPOLSKI, 2007) relata que a empresa de telecomunicações Comcast usou o aplicativo Sandvine[4] para gerenciar conexões P2P, e explica como ela fazia isto: (i) o aplicativo Sandvine lia os pacotes que estavam atravessando a fronteira da rede Comcast; (ii) se o aplicativo detectava que o tráfego de saída P2P era maior do que um limite determinado pela Comcast, o Sandvine começava a interromper as sequências de pacotes; e (iii) a interrupção era realizada através do envio de um pacote TCP forjado (com identificação de *peer*, porta e sequência de numeração correta) mas incluindo a *flag* RST (*reset*) do TCP. Este pacote interrompia a comunicação.

Em abril de 2009, James Kendrick (KENDRICK, 2009) denunciou que o operador T-Mobile, da Alemanha, estava proibindo o uso do programa Skype em suas redes. O autor relata que o bloqueio de todas as aplicações de VoIP estava ocorrendo através da rede móvel da T-Mobile por dois anos. E ainda, de acordo com o autor, os motivos alegados pela T-Mobile foram puramente técnicos e não econômicos: (i) segundo a explicação dada, o nível elevado de tráfego prejudicaria o desempenho da

[3]https://wiki.vuze.com

[4]https://www.sandvine.com

rede da T-Mobile, e (ii) se o Skype não funcionasse corretamente, os clientes então responsabilizariam a T-Mobile pelo problema.

Em junho de 2009, a FNN (*Fast Net News*) publicou que a BT, a empresa britânica de telecomunicações, estava estrangulando todos os vídeos da BBC porque a BT limitava a taxa de *streaming* de vídeo a 896 Kbps. O motivo alegado pela BT foi que o crescimento do tráfego de vídeo aumentou seus custos (BT..., 2015).

Em 2010, Fei-Yang Ling e outros autores, analisaram o bloqueio do BitTorrent efetuado pela Comcast, e qual foi o motivo deste bloqueio. Nesta análise, os autores argumentam e concluem que, embora a Comcast tenha afirmado que o bloqueio ocorreu para garantir a qualidade de serviço adequada aos outros usuários da rede, a razão do bloqueio foi, na verdade, financeira. Segundo os autores, o bloqueio ocorreu porque os ISPs não podem cobrar dos provedores de conteúdo um preço para o acesso preferencial aos seus serviços. Os autores concluem que este benefício não deve ser obtido por meio da violação à Neutralidade da Rede. Concluem também que as aplicações P2P não degradam a qualidade das redes, elas simplesmente transferem a responsabilidade dos fornecedores de conteúdo para os ISPs (LING et al., 2010).

Em fevereiro de 2011 foi lançado o *siteGreatFirewall.biz*. Por meio dele foi dado início à coleta de dados sobre o Grande *Firewall* da China, tornando esta informação pública. Em outubro de 2011 o nome do *site* mudou para *GreatFire.org* que desde então continua a adicionar informações sobre *sites* e palavras-chave bloqueados na China. Atualmente este *site* monitora mais de 10.000 URLs. Devido ao regime político da China e a natureza do *site* ele é mantido de forma anônima, por uma organização sem fins lucrativos, coletando e compartilhando as informações em tempo real. Além disso, o *site* mantém também o histórico sobre *sites* e pesquisas bloqueados, com um foco particular no Google e no Baidu. Os dados são coletados das seguintes maneiras: (i) adições por usuários: qualquer usuário pode adicionar uma nova URL para testes e ela será continuamente testada pelo sistema; e (ii) adições por colaboradores: qualquer URL que esteja marcada como bloqueada na China por fontes como *Autoproxy*, *China Digital Times* e Herdict, é automaticamente importada para dentro do sistema. Cada palavra-chave no sistema, seja no Baidu, Google, Wikipedia ou Weibo, corresponde a uma URL sobre a qual o *site* é testado para a censura. Essas palavras-chave são adicionadas principalmente pelos usuários. O *China Digital Times* tem uma extensa lista de palavras-chave bloqueadas ou sensíveis, e todas elas foram integradas ao sistema.

De acordo com as estatísticas disponibilizadas no *siteGreatFire.org*, o resultado do monitoramento sobre o bloqueio efetuado pelo governo na China mostra que: (i) dos 45.039 domínios analisados, 5.941 foram bloqueados (ii) das 18.364 buscas Google analisadas, todas foram bloqueadas; (iii) dos 834 *sites* Google analisados, 748 foram bloqueados; (iv) dos 18.887 *sites* acessados de forma segura com HTTPS analisados, 4.707 foram bloqueados; (v) dos 18.052 endereços IP analisados, 8.234 foram bloqueados; (vi) das 240.295 URLs analisadas, 65.338 foram bloqueadas; (vii) das 27.625 buscas Weibo analisadas, 3.193 foram bloqueadas; e (viii) das 1.216 páginas da Wikipédia analisadas, 874 foram bloqueadas (ONLINE..., 2015).

Em abril de 2011, os autores da ferramenta CensMon fizeram testes utilizando *testbed* do PlanetLab. Mais precisamente, implantaram 174 agentes em 33 países diferentes (141 *ASes* distintos, 130 cidades distintas) no PlanetLab. Todas as medidas de avaliação foram realizadas durante um período de 14 dias. Neste período o CensMon testou 4.950 URLs únicas a partir de 2.500 domínios e detectou que 951 URLs foram filtradas em 193 domínios. Após testarem manualmente estes 193 domínios relatados como censurados, a fim de verificar se havia falsos positivos, descobriram que três deles foram falsamente marcados. O nó do agente chinês relatou o maior número de filtragens, tendo 176 domínios marcados como censurados (SFAKIANAKIS; ATHANASOPOULOS; IOANNIDIS, 2011).

O *site* europeu Respect My Net[5] foi lançado em 22 de setembro de 2011 para os usuários da Internet poderem relatar as violações da Neutralidade da Rede. Este *site* traz uma lista de todos os casos notificados, com confirmações e provas oferecidas pelos usuários. Os casos não considerados como violações da Neutralidade da Rede, sob as diretrizes do *site*, são removidos ou não são validados. O *site* traz um total de 219 relatos confirmados que envolvem 18 países da Europa e 71 operadores. A lista dos relatos contém, além do país, o operador e o status da verificação de confirmação. A lista contém também o tipo do contrato firmado entre o usuário e o operador, o tipo da violação, e se ocorreu na rede fixa ou móvel. Além disso, a lista traz qual foi o recurso afetado, como: VOIP; P2P; FTP; YouTube; Skype; e DNS. E, ainda, a lista informa se a violação ocorreu em toda a Internet ou em uma página específica, e quantas confirmações aquela reclamação recebeu de outros usuários. Nos anos de 2011 e 2012 foram três os casos em destaque: (i) o estrangulamento do YouTube na França, pelo

[5]https://respectmynet.eu

operador Free (rede fixa, cabeada), com a confirmação de 431 usuários; (ii) o bloqueio DNS (*Domain Name System*) para o *sitethepiratebay.org* na Bélgica, pelo operador Mobile Vikings (rede móvel) com a confirmação de 18 pessoas; e (iii) o bloqueio da porta 25 para todos os serviços SMTP (*Simple Mail Transfer Protocol*), exceto os da própria Belgacom, da Bélgica, pelo operador Belgacom (rede fixa, cabeada) com a confirmação de 21 pessoas (RESPECT..., 2015).

Em 2012 foi publicada no *Telecommunications Policy* uma análise sobre os casos de uso de DPI por operadores de rede nos EUA e no Canadá. Esta análise foi efetuada com o objetivo específico de detectar o bloqueio ou estrangulamento do tráfego P2P de compartilhamento de arquivos. Os autores usaram os dados extraídos da ferramenta Glasnost para efeitos de comparação (MUELLER; ASGHARI, 2012).

Os autores da ferramenta Adkintun (descrita no Capítulo 4) apresentaram três casos sobre o seu uso no Chile, entre os anos de 2011 e 2013 (BUSTOS-JIMÉNEZ; FUENZALIDA, 2014), descritos a seguir. O primeiro caso é o da VTR e Movistar. A pedido da SUBTEL, agência reguladora de telecomunicações do Chile, a ferramenta foi usada para analisar o comportamento destes dois ISPs que, juntos, controlam em torno de 80% dos serviços de banda larga fixa no Chile. Ao verificar os dados coletados, notou-se que durante a noite a velocidade de *download* na Internet diminuiu, ficando bem abaixo do contratado para todos os planos de Internet das duas empresas. Todas as conclusões foram informadas para a SUBTEL. O segundo caso envolveu a defesa dos direitos dos usuários. Em 11 de setembro de 2012, o Canal Nacional de TV Pública transmitiu uma reportagem especial sobre o primeiro caso descrito acima. A reportagem revelou os problemas com os provedores de Internet de banda larga e o quanto os ISPs chilenos cumpriam seus contratos de serviço. Após esta reportagem em TV nacional, notou-se que o número de reclamações dos usuários para a SUBTEL aumentou.

O terceiro caso é sobre o efeito bumerangue da Adkintun. Em 18 de junho de 2013, uma ONG denominada Civico entrou com uma ação contra a SUBTEL por prevaricação, apresentando relatórios públicos com base nos dados coletados pelos autores da Adkintun. Estes relatórios foram usados como prova de que a SUBTEL não processou nem iniciou ações de auditoria contra os ISPs chilenos, apesar das reclamações recebidas. Como resultado, a Câmara dos Deputados do Chile decidiu solicitar à SUBTEL todos os procedimentos para fazer cumprir a Lei da Neutralidade da Rede chilena. De acordo com os autores da Adkintun, este é o primeiro caso sobre uma infraestrutura ter sido exigida por uma agência governamental, a fim de preservar os

direitos estabelecidos na Lei de Neutralidade da Rede, e que, depois, foi usada contra esta mesma agência governamental. O projeto Adkintun foi totalmente implantado e tem recolhido dados desde setembro de 2011, e foi usado por mais de 10.000 usuários. O Adkintun Mobile, em sua nova versão lançada no Chile em março de 2014, foi instalado em 110 dispositivos diferentes e desde então teve quase 25 milhões de eventos recolhidos (LALANNE et al., 2015).

A ferramenta HAKOMetar (descrita no Capítulo 4) foi usada por usuários finais na Croácia entre novembro de 2012 e março de 2013, e o número total de medições excedeu 25.000. Do número total de medições realizadas, aproximadamente 5.000 foram validadas e, dos ciclos de medição realizados, aproximadamente 80 ciclos completos foram aceitos como válidos. Do número total de ciclos completos, várias dezenas deles obtiveram, como resultado, medidas de velocidades que estavam bem abaixo do mínimo da velocidade contratada. Este resultado fundamentou as queixas dos usuários contra 3 dos 16 operadores analisados. Os documentos impressos dos resultados de medição obtidos pela HAKOMetar foram anexados às queixas. O resultado destas queixas foi positivo para os usuários finais (WEBER et al., 2013).

Em janeiro de 2013, num fórum de discussão do Google, usuários relatam teste de velocidade feito com o *speedtest.net*. De acordo com o teste, afirmaram ter contratado uma velocidade de 10 Mbps ou de 40 Mbps. Entretanto, quando tentaram assistir vídeos do YouTube, a velocidade tornou-se lenta, com os vídeos chegando por vezes a levar 10 minutos para iniciar, ou não iniciando, o que os levou a acreditar que estava havendo estrangulamento por parte de seus ISPs (GOOGLE, 2013).

Em seu artigo de 18 de junho de 2013, Collin Anderson descreve a detecção de estrangulamento de BitTorrent usando os dados coletados em clientes no Irã, por meio da ferramenta NDT (*Network Diagnostic Tool*). Como resultado, o autor encontrou dois períodos significativos e períodos estendidos de estrangulamento potencial, dentro do conjunto de dados, ocorridos entre 30 de novembro de 2011 e 15 de agosto de 2012. Neste período, o autor verificou uma diminuição de 77% na taxa de transferência de *download*. E, no período compreendido entre 04 de outubro e 22 de novembro de 2012, o autor verificou uma diminuição de 69% (ANDERSON, 2013).

Em 24 de junho de 2013, leitores do jornal *online* da Zâmbia, chamado *Zambianwatchdog.com*, relataram problemas. O Zâmbia Watchdog é considerado o maior *site* na Zâmbia, após o Facebook, o Google e o YouTube. Testes foram então executados com a ferramenta Ooni. Estes testes revelaram que o Zâmbia Watchdog era

o único *site* bloqueado devido a filtragem e uso de DPI, feitos pelo governo zambiano (ZAMBIA..., 2013).

A tese de doutorado de 2013 de Ravinder Shankesi (SHANKESI, 2013) traz a proposta de uma infraestrutura para detecção de manipulação de rede chamada *Friendsourcing.* Esta proposta baseia-se numa espécie de *crowdsourcing*, na qual os indivíduos usam suas redes sociais para obter a ajuda de seus amigos, a fim de detectar se estão sofrendo interrupção acidental ou manipulação deliberada na rede. Para testar sua proposta, o autor implantou a ferramenta SiteViews, uma aplicação baseada em *web-browser* para detectar manipulação de tráfego baseado na *web*. O autor realizou a pesquisa de campo com 54 usuários reais na Índia, os quais foram selecionados a partir de um par inicial de usuários. O resultado detectou 64 URLs distintas bloqueadas dentro de vários ISPs na Índia, bem como vários tipos de mecanismos de bloqueio usados em 13 ISPs diferentes na Índia. O resultado mostrou também que os *sites* que oferecem *links* para *torrents* foram frequentemente bloqueados por todos os principais ISPs deste estudo.

Também de 2013, é a dissertação de Shadi Esnaashari (ESNAASHARI, 2014). Esta dissertação traz a ferramenta WCMT (*Web Censorship Monitoring Tool*). Esta ferramenta foi utilizada entre julho e setembro de 2013, para identificar bloqueio de acesso a páginas Web e serviços da Internet na rede de diferentes organizações e ISPs em Wellington, na Nova Zelândia. Os resultados mostraram que todas as organizações e ISPs avaliados efetuaram bloqueio de algum conteúdo. Porém, houve uma variedade grande de conteúdos diferentes bloqueados em redes diferentes. O autor afirma que isto demonstra a falta de critérios das organizações ao definirem o que deve ser bloqueado.

Em 10 de fevereiro de 2014, o *site* de mídia social *reditt*, onde os membros registrados podem publicar mensagens, recebeu uma mensagem sobre a ocorrência de degradação de desempenho de uma VPN usando a porta padrão OpenVPN, indicando possivelmente intervenção indevida do ISP. Esta ocorrência em seguida recebeu confirmação de outros usuários (I JUST..., 2014).

Em outro caso, também de 10 de fevereiro de 2014, Jon Brodkin, relata no *site* da Ars Technica, que a velocidade do Netflix apresentou queda nas redes Verizon e Comcast nos três a quatro meses anteriores (BRODKIN, 2014).

Além disso, também em 2014, foi desenvolvida na Noruega uma infraestrutura dedicada para medições e experimentação em redes de banda larga móveis. Esta infraestrutura, denominada NNE (*NorNet Edge*), consiste em mais de 400 nós

distribuídos geograficamente por toda a Noruega. A implantação dos nós NNE ocorreu em colaboração com o governo devido ao interesse pela votação eletrônica. O recenseamento eleitoral é feito eletronicamente, e todas as centrais de voto devem ter uma conexão de Internet. Deste modo, os nós NNE são usados para monitorar a conexão Internet existente nesses locais de voto, e para fornecer uma conexão robusta de *backup*, no caso da conexão principal falhar (KVALBEIN et al., 2014). Durante o período de um mês, ao longo de novembro 2014, foi feito um estudo em grande escala com a NNE para medir atrasos de ida e de volta em duas operadoras móveis na Noruega. Este estudo utilizou ambos nós de medição, fixos e móveis, um total de 200 nós distribuídos geograficamente. Como resultado, os autores verificaram uma alta variação de atraso dentro do mesmo tipo de acesso. Em ambas as redes estudadas, os autores mediram os atrasos de ida e de volta, várias vezes por hora. Verificaram que os atrasos foram mais frequentes quando os nós estavam se movendo. Investigando os episódios de atrasos extremos, descobriram que eles foram causados pelas políticas de bufferização, além de características da própria rede física utilizada. Este resultado leva a crer que, neste caso específico, não houve quebra da Neutralidade da Rede em si (LARSON, 2015).

Em 15 de dezembro de 2015 foi divulgado que a FCC recebeu mais de 13.000 queixas dos usuários do plano Xfinity da Comcast devido ao uso de barreiras que limitam o uso de dados (RISLEY, 2015).

Em 2016 proliferaram os casos de denúncia quanto às violações da Neutralidade da Rede. Os casos a seguir foram selecionados para serem apresentados aqui, de acordo com a diversidade da violação e dos agentes envolvidos. Em 1º de fevereiro de 2016, Barbara van Schewick, envia ao Presidente da FCC, Tom Wheeler, um relatório. Neste relatório, ela aponta que o serviço Binge On do operador T-Mobile viola os princípios fundamentais da Neutralidade da Rede e prejudica a escolha do usuário, a inovação, a concorrência e a liberdade de expressão *online*. Segundo a autora, em novembro de 2015, a T-Mobile, o terceiro maior provedor de acesso à Internet móvel nos EUA, lançou o serviço Binge On. Neste serviço, o operador oferece *streaming* ilimitado de vídeo a partir de provedores selecionados. Com o Binge On, os clientes podem receber vídeo de quarenta e dois provedores, como Netflix, Amazon, Hulu, HBO, e outros, sem o uso dos seus planos de dados, uma prática conhecida como “taxa zero”. Para a autora, o Binge On prejudica a visão central da Neutralidade da Rede, porque os ISPs que

conectam os usuários à Internet não devem agir como *gatekeepers*, favorecendo algumas aplicações em detrimento de outras (VAN SCHEWICK, 2016).

Em 7 de fevereiro de 2016, o operador Verizon foi acusado de violar os princípios da Neutralidade da Rede com seu serviço móvel de vídeo chamado Go90. Com este serviço de taxa zero a Verizon exclui o seu próprio serviço de *streaming* de vídeo móvel da franquia de dados de seus clientes (LOMAS, 2016).

Em 2 de março de 2016, o grupo de interesse público sem fins lucrativos, *Public Knowledge*, entrou com uma queixa junto à FCC a respeito do serviço *Stream* TV da Comcast. A denúncia diz que a Comcast não inclui o tráfego *Stream* TV na sua própria franquia de dados. De acordo com a *Public Knowledge*, isto é tanto uma violação do acordo de fusão da Comcast com a NBC-Universal, quanto é contra a normativa da Internet aberta da FCC. O serviço *Stream* TV é uma oferta para os clientes Xfinity Internet, que inclui canais locais, HBO, e o uso de uma nuvem (DREIER, 2016). Por conseguinte, a Public Knowledge solicita que a FCC impeça a continuidade da oferta deste serviço discriminatório de taxa zero da Comcast, impeça seu uso discriminatório de franquia de dados, e tome quaisquer outras ações de controle que considerar necessárias. Além disso, a Public Knowledge solicita que a FCC coloque fim a este comportamento e evite que ele se repita no futuro. A Public Knowledge fez estas solicitações à FCC, considerando que a Comcast já é um distribuidor de vídeo dominante no mercado, e o maior provedor de banda larga do país, e que a Comcast, com este serviço, está tomando passos para expandir ainda mais a sua posição dominante em novos mercados, como o mercado de vídeo *online* (FCC, 2016b). Em 14 de março de 2016, a Comcast responde que o serviço *Stream* TV não é um serviço OTT (*over-the-top*), serviço de vídeo *online*, ou entregue através da Internet, ao contrário, é um serviço de cabo. Ressalta que, assim como todos os outros serviços de cabo da Comcast, este serviço é entregue às casas dos clientes através da rede privada (da Comcast) sobre os sistemas de cabo da Comcast. E finaliza dizendo que este serviço está sujeito e cumpre com todos os requisitos regulamentares (FCC, 2016a).

Em 24 de março de 2016, a Netflix postou em seu *blog* que, em um esforço para proteger seus clientes da cobrança adicional quando excedem a franquia de dados móveis, estabeleceu como taxa padrão de *bits* para visualização, através de redes móveis, 600 Kbps. Segundo a Netflix, esta medida trata de um equilíbrio que garante uma boa experiência de transmissão, evitando multas não planejadas de provedores móveis (SQUEO, 2016). Desta forma, a Netflix assume que faz estrangulamento

colocando barreiras em seus fluxos, tornando-os muito mais lentos do que o que deveria ser possível nas redes sem fio atuais. Em 25 de março de 2016, a ACA (*American Cable Association),* um grupo que representa mais de 900 pequenas e médias empresas de cabo, escreve que está "decepcionada, mas não surpresa", que a Netflix use sua imunidade às regras da Neutralidade de Rede da FCC para se envolver nessa prática. Diante disso, a ACA solicita à FCC que inicie um inquérito sobre as práticas dos provedores de conteúdo e como essas empresas podem ameaçar a abertura da Internet. Para a ACA, a FCC tem a autoridade para conduzir tal investigação e emitir regulamentos, caso seja considerado necessário. A ACA conclui que a abordagem da FCC para a Neutralidade da Rede é unilateral e injusta, porque deixa os consumidores desprotegidos das ações dos provedores de conteúdo, que bloqueiam e regulam o tráfego legítimo (AMERICAN CABLE ASSOCIATION, 2016).

Também sobre este caso, em 28 e 29 de março de 2016, Jon Brodkin, da Ars Technica, aponta que a Netflix poderia ter sido mais transparente sobre o seu estrangulamento e como ele é aplicado. Para o autor, a Netflix estaria estrangulando tráfego em redes móveis há mais de cinco anos sem revelar o sistema. E, ainda, o autor ressalta que este estrangulamento aparentemente se aplicou até mesmo para clientes da AT&T e da Verizon, que pagam para dados ilimitados ou planos de dados maiores do que a média (BRODKIN, 2016a, 2016c). E, finalmente, também sobre este caso, Michael O'Rielly, membro da FCC, disse em seu discurso de abertura do Fórum de Ação Americana, em 29 de março de 2016, que a Netflix não violou as regras da Neutralidade da Rede da FCC, promulgada em fevereiro de 2015, e que estas regras só se aplicam aos ISPs, e não aos provedores de conteúdo independentes, como a Netflix. Portanto, segundo ele, não há violação de Neutralidade da Rede para explorar. Entretanto, em seu discurso, ele também ressaltou que a Netflix fez acusações de irregularidades cometidas por ISPs, ao mesmo tempo em que sabia que as suas próprias práticas eram uma das causas de degradação dos vídeos recebidos por consumidores, reconhecendo que a Netflix não foi um participante passivo quando participou do processo de estabelecimento das regras da Neutralidade da Rede. Dito de outro modo, Michael O'Rielly salienta que a Netflix foi uma representante chave do suposto mercado no qual as regras foram concebidas para proteger o negócio de distribuição de vídeo. Muitas regras foram baseadas nas representações feitas pela Netflix e outras entidades em situação semelhante, incluindo o Google. Para ele, as regras para acordos de troca de tráfego foram baseadas no medo de práticas anticompetitivas e na interferência desleal

de *gatekeepers* pelos ISPs, termo inventado pela Netflix. E, no entanto, ao mesmo tempo em que a Netflix estava fazendo estas reivindicações, teve um comportamento que pode ser considerado incoerente. E conclui que, deste modo, estas revelações põem em dúvida todo o fundamento e a razão de ser da decisão da Neutralidade da Rede (O'RIELLY, 2016).

Em 1º de abril de 2016 um grupo de mais de 50 organizações de interesse público, e de defesa do consumidor nos EUA, escreveram uma carta ao presidente da FCC contra a prática da taxa zero. Dentre estas organizações estão: a *Electronic Frontier Foundation*, a *Free Press*, a *New America's Open Technology Institute*, e a *Rural Broadband Policy Group*. Esta carta destaca as práticas de taxa zero da Verizon, da AT&T e da T-Mobile, que distorcem a concorrência, sufocam a inovação, limitam a escolha do usuário, e elevam preços (CAMPBELL, 2016).

2.5. CONSIDERAÇÕES FINAIS

Observa-se nos estudos de caso apresentados, que as denúncias ocorreram pelos motivos mais variados, e nos mais diversos lugares. Da mesma forma, estas queixas ocorreram ao longo de todo o período de debate, incluindo países com e sem normatização. Isso revela as dificuldades dos órgãos reguladores em fiscalizar as ações dos ISPs, ao mesmo tempo em que demonstra que os ISPs relutam em acatar as regras estabelecidas. Os estudos de caso relatados revelam que os ISPs detêm poder político e econômico em medida mais que suficiente para seguirem exercendo o papel de opositores no debate, com o intuito de obstruir a efetividade da Neutralidade da Rede. O grande número de estudos de caso em 2016 confirma a atualidade do debate e o seu estado contínuo de ebulição.

CAPÍTULO III

PANORAMA MUNDIAL DA NORMATIZAÇÃO DA NEUTRALIDADE DA REDE

O objetivo deste capítulo é fornecer um panorama mundial sobre a normatização da Neutralidade da Rede. A metodologia utilizada para a organização do capítulo é a seguinte. Adotou-se como termo genérico a palavra normatização, para qualquer estabelecimento de regras, princípios ou Leis, que foram instituídos nos países em prol da Neutralidade da Rede. A normatização pode ter sido estabelecida pela presidência do país, por algum órgão governamental federal representativo, como um ministério, por exemplo, ou, ainda, esta normatização pode ter sido estabelecida diretamente pelo ente regulador governamental, responsável pela regulação das telecomunicações no país, ou na União Europeia, como é o caso do BEREC.

Para estabelecer o panorama mundial, foi selecionada a União Europeia para representar a Europa, porque engloba 28 países. E, ainda, para ampliar o quadro representativo da Europa, foram selecionadas também a Noruega e a Rússia, países que não são membros da União Europeia. Para representar a América, foram selecionados o Canadá, o Chile, a Colômbia, o Brasil, o México, e os Estados Unidos. Para representar a Ásia, foram selecionados o Japão, a Coréia e a Índia. Para representar a Oceania foram selecionadas a Nova Zelândia e a Austrália e, para representar a África, foram selecionados a África do Sul e o Quênia.

A seleção ocorreu de forma natural durante a pesquisa, conforme foi possível encontrar as informações necessárias, nas bases de dados bibliográficas, nos *sites* das agências reguladoras, nos *sites* de outros órgãos dos governos dos países e, ainda, nos *sites* de notícias. Embora este estudo não pretenda ser exaustivo, buscou-se aprofundar a pesquisa quanto aos principais fatos ocorridos em determinados países. Um deles são os Estados Unidos, considerando que foi onde se deu início ao debate, e onde se criou o termo Neutralidade da Rede, embora não tenha sido o primeiro país a obter a normatização desta matéria. O outro é a União Europeia, considerando que é o organismo responsável pela representação política e econômica de 28 países

independentes, chamados de Estados-membros. E, considerando também, que a União Europeia busca a uniformização na normatização da Neutralidade da Rede, com o estabelecimento de regras únicas para todos os seus Estados-membros. E, ainda, o outro país é o Brasil, por ser este o país de origem desta autora e, principalmente, porque o objetivo geral da presente tese é propor um observatório de Neutralidade da Rede no Brasil, o que acarreta para tanto, aprofundar a pesquisa sobre o tema neste país.

A ordem adotada para a apresentação do panorama da normatização é cronológica. Nesta apresentação destaca-se em cada país, a maneira encontrada para normatizar a Neutralidade da Rede, os principais pontos ou eventos que levaram à normatização e, o que de fato, foi estabelecido para que os usuários tenham acesso a uma Internet neutra.

Para a elaboração da Figura 2, que traz a Linha do Tempo da normatização, apresentada ao final do capítulo, levou-se em conta somente os anos nos quais efetivamente a normatização foi instituída de alguma forma, impulsionando o avanço do debate. Desconsiderou-se, portanto, na elaboração desta figura, as particularidades ocorridas ao longo do processo, tais como as consultas públicas, os litígios entre órgãos governamentais e ISPs, e a criação de comissões governamentais de trabalho para estudo do tema, embora estes eventos estejam retratados no texto, devido à sua importância no processo da normatização.

O debate da Neutralidade da Rede permanece controverso e em ebulição em vários países. Este fato impôs que fosse tomado um marco temporal de encerramento da pesquisa e, para isto, foi adotado o dia 1º de maio de 2017. Entretanto, restam exceções, como a pesquisa sobre o tema no Brasil, que seguiu além desta data, para ser tratado novamente no Capítulo 5.

É importante salientar que não foi encontrada padronização no debate que levou à normatização da Neutralidade da Rede nos países selecionados. Cada país mostrou ter peculiaridades próprias ao longo do processo de instituição da normatização, o que trouxe algumas dificuldades na obtenção da interpretação adequada aos textos que contêm estas particularidades. Entretanto, ainda que pesem algumas dificuldades encontradas na tradução dos textos, para melhor interpretação das peculiaridades, a maior dificuldade encontrada deveu-se ao entendimento adequado, pela tradução pura dos textos, àquelas peculiaridades relativas às características jurídicas de alguns países.

É importante salientar também que, conforme exposto nos capítulos anteriores, em um ambiente sem normatização, os ISPs têm autonomia para decidir como devem

efetuar o gerenciamento do tráfego de suas redes. Porém, esta decisão tomada pelos ISPs pode acarretar algum tipo de prejuízo aos usuários finais e ser nociva para a manutenção da Internet, conforme ela foi concebida. Seguindo esta linha de raciocínio, somente em um ambiente normatizado as ferramentas de monitoramento do tráfego efetuado pelos ISPs poderão ser úteis e efetivas, atingindo o objetivo de detectar violações da Neutralidade da Rede. Do mesmo modo, somente a partir do resultado positivo de alguma violação, fornecido pelo uso das ferramentas de detecção de violações da Neutralidade da Rede, é que os agentes de controle dos governos, responsáveis pela fiscalização da área das telecomunicações, poderão tomar as providências cabíveis, a fim de punir ou coibir tais práticas proibidas aos ISPs.

Para apresentar o panorama mundial sobre a normatização da Neutralidade da Rede, conforme aqui proposto, este capítulo é subdividido em 15 seções: 3.1. Japão; 3.2. Noruega; 3.3. Canadá; 3.4. Chile; 3.5. Colômbia; 3.6. Coréia; 3.7. Nova Zelândia; 3.8. Rússia; 3.9. Brasil; 3.10. México; 3.11. EUA; 3.12. Índia; 3.13. União Europeia; 3.14. Austrália; 3.15. África do Sul e Quênia; 3.16. Considerações Finais.

3.1. JAPÃO

Em 19 de setembro de 2006, o Japão, por meio do MIAC (*Ministry of Internal Affairs and Communications*), lança o Programa de Promoção da Nova Concorrência 2010 (*New Competition Promotion Program* 2010). Este programa teve como base a disseminação das redes e a criação de um Grupo de Trabalho sobre a Neutralidade da Rede. O Grupo de Trabalho foi criado para elaborar o arcabouço (*framework)* necessário para a Neutralidade da Rede (MIAC, 2006). O Grupo de Trabalho concluiu em seu primeiro relatório, de 20 de setembro de 2007, que a Neutralidade da Rede, com o desenvolvimento de redes baseadas em IP era, de fato, a equidade (*fairness*) no uso das redes (a neutralidade das camadas responsáveis pelo tráfego de dados), e a equidade dos custos das redes, adotando um modelo de partilha de custos. Após isto, usando a Neutralidade da Rede como um pressuposto básico, o grupo selecionou e organizou tópicos para pesquisar medidas competitivas. Esta pesquisa contou com a participação dos principais agentes de todas as áreas envolvidas (MIAC, 2007).

Em 07 de março de 2008, o grupo publicou então o relatório onde consta o "Roteiro de Investigação para a Manutenção da Neutralidade da Rede", que contém as

seguintes recomendações, que visam reforçar os pressupostos estabelecidos em 2007 (MIAC, 2008): (i) equidade dos custos de rede. Influenciam este modelo aspectos como o congestionamento de rede; desenvolvimento de tecnologias de distribuição de conteúdo usando P2P; e certificação de QoS para os ISPs. (ii) obtenção de uma compreensão mais detalhada sobre o tráfego da Internet. Influenciam esta compreensão aspectos como reforço na capacidade de resolução de litígios, incluindo a Alternativa de Resolução de Litígios ADR (*Altemative Dispute Resolution*). (iii) equidade no uso da rede, incluindo prevenção de abuso de posição dominante no mercado; e formulação de regras para interconexão de Redes de Nova Geração (*Next Generation Networks* (NGNs)) da *Nippon Telegraph and Telephone Corporation* (NTT). (iv) revisão da regulação dominante. Mudança para um arcabouço de regulamentos que possam lidar com questões como a consolidação do mercado, fazendo uso dos resultados da avaliação da concorrência quando o domínio do mercado foi reconhecido; reconhecimento de alavancagem nos mercados vizinhos e posições dominantes de mercado; e o fortalecimento do monitoramento do mercado. (v) outras medidas, como a promoção da diversificação das redes de acesso, incluindo suporte de construção de redes por organismos regionais, e promoção da BWA *(Broadband Wireless Access*); a revisão do sistema legal para abarcar novos modelos de negócio (incluindo uma investigação da legislação de fusão); e a investigação de medidas para proteger os usuários.

3.2. NORUEGA

A Noruega, que não faz parte da União Europeia como Estado-membro, lançou em 24 de fevereiro de 2009 suas diretrizes para a Neutralidade da Rede, por meio de seu órgão regulador, a NPT (*Norwegian Post and Telecommunications Authority* - atualmente renomeada como Nkom, *Norwegian Communications Authority*). Os princípios ou diretrizes estabelecidos foram os seguintes: (i) os usuários da Internet têm direito a uma ligação à Internet com uma capacidade e uma qualidade pré-definidas. (ii) os usuários da Internet têm direito a uma ligação à Internet que lhes permita: enviar e receber conteúdos da sua escolha; utilizar serviços e executar aplicativos de sua escolha; conectar hardware e usar software de sua escolha que não danifiquem a rede; e (iii) os usuários da Internet têm direito a uma ligação à internet que esteja livre de

discriminação, no que diz respeito ao tipo de aplicação, ou serviço, ou conteúdo, ou com base no endereço do remetente ou do destinatário. (NETWORK..., 2009). Em 2013, a Nkom reitera que o modelo norueguês para a Neutralidade da Rede pode ser descrito como uma abordagem de corregulação, de modo que o regulador é capaz de definir objetivos claros para as orientações que serão desenvolvidas, enquanto, ao mesmo tempo, os vários intervenientes da indústria podem equilibrar os pontos de vista de cada um. A Nkom considera que há três principais tipos de *players* nesta indústria: (i) os prestadores de serviços de Internet, (ii) os provedores de conteúdo e aplicativos, e (iii) os consumidores, representados pelas organizações de consumidores.

Para a Nkom, desde 2009 as orientações têm funcionado como deveriam na Noruega, e nenhuma atualização é necessária (NKOM, 2013). Em 18 de novembro de 2014, Frode Sørensen, Conselheiro Sênior da Nkom, publica na página da Nkom, um texto no qual explica as diretrizes norueguesas para a Neutralidade da Rede. Ressalta que estas diretrizes, claramente evidenciam que os usuários da Internet têm direito a receber uma conexão à Internet que seja livre de discriminação, em relação ao tipo de aplicação, serviço ou conteúdo, ou com base no remetente ou no recebedor. Isto significa que no mercado norueguês, a prática da taxa zero constitui uma violação das orientações. Frode Sørensen enfatiza que, à primeira vista, pode parecer que todo o tráfego é tratado igualmente neste modelo de tarifação (*charging model*), mas o fato é que após o usuário ter usado a sua cota ou franquia, o tráfego que está isento será permitido a continuar, enquanto todos os outros tráfegos serão estrangulados ou bloqueados. Conclui que este é, claramente, um caso de discriminação entre os diferentes tipos de tráfego. E finaliza, ressaltando que a Internet é importante para a economia, para a diversidade cultural, para a vida social e para a democracia e, portanto, a NKom trabalha para preservar a Internet como uma plataforma aberta (SØRENSEN, [2014b]).

3.3. CANADÁ

Em 21 de outubro de 2009, o Canadá, por meio da CRTC (*Canadian Radio Television and Telecommunications Commission*), expõe as suas determinações em relação ao uso de práticas de gerenciamento do tráfego da Internet pelos ISPs. A Comissão estabelece uma abordagem baseada em princípios que equilibram

apropriadamente a liberdade dos canadenses de utilizar a Internet para várias finalidades, com os interesses legítimos dos ISPs de gerenciar o tráfego gerado em suas redes. Isto de acordo com a legislação, incluindo a legislação de privacidade.

A CRTC baseou suas determinações em quatro considerações conforme segue. (i) Transparência. A utilização de quaisquer práticas de gerenciamento de tráfego de Internet pelos ISPs deve ser transparente. (ii) Inovação. O investimento na rede é uma ferramenta fundamental para lidar com o congestionamento, por exemplo, e deve continuar sendo a principal solução utilizada pelos ISPs; no entanto, o investimento por si só não elimina a necessidade de certas práticas de gerenciamento de tráfego na Internet. (iii) Clareza. Os ISPs devem assegurar que quaisquer práticas de gerenciamento de tráfego de Internet que empregarem, não sejam injustamente discriminatórias e nem indevidamente preferenciais. (iv) Neutralidade concorrencial. Para os serviços de varejo, os ISPs podem continuar a empregar práticas de gerenciamento de tráfego da Internet sem a aprovação prévia da Comissão. A CRTC destaca que irá rever essas práticas, avaliando-as com base em preocupações decorrentes principalmente de queixas de consumidores. Para os serviços "de atacado" haverá um exame complementar. Quando um ISP empregar práticas de gerenciamento de tráfego da Internet mais restritivas para os seus serviços "de atacado" do que para os seus serviços "de varejo", será necessária a aprovação da Comissão para implantar essas práticas. Práticas de gerenciamento de tráfego da Internet, aplicadas aos serviços "de atacado", devem respeitar o arcabouço das práticas de gerenciamento de tráfego da Internet, e não devem ter um impacto significativo e desproporcionado para o tráfego secundário do ISP (CRTC, 2009).

3.4. CHILE

O governo do Chile promulgou a Lei 20.453, em 18 de agosto de 2010. Nela, o governo chileno consagra expressamente o princípio da Neutralidade da Rede para os consumidores e usuários da Internet. Esta Lei estabelece as seguintes regras para as concessionárias de serviço público de telecomunicações (que prestam serviço aos provedores de acesso à Internet), e também para os provedores de acesso à Internet, que prestam serviços comerciais de conectividade para os usuários. (i) Não podem arbitrariamente bloquear, interferir, discriminar, impedir ou restringir o direito de

qualquer usuário da Internet em usar, enviar, receber ou oferecer qualquer conteúdo, aplicação ou serviço legal através da Internet, e qualquer outra atividade ou uso legal através da rede. (ii) Não podem limitar o direito de um usuário de inserir ou usar qualquer classe de instrumentos, equipamentos ou dispositivos na rede, desde que sejam legais e que não danifiquem ou prejudiquem a qualidade ou serviço da rede. (iii) Deverão fornecer as expensas dos usuários que os solicitem, serviços de controles parentais para conteúdos que violem a lei, a moral ou os bons costumes, sempre e quando o usuário seja informado com antecedência e de maneira clara e precisa a respeito do alcance de tais serviços. (iv) Deverão publicar em seu *site*, toda a informação relativa às características do acesso à Internet oferecido, sua velocidade e qualidade de conexão, diferenciando entre as conexões nacionais e internacionais, bem como a natureza e garantias do serviço (CHILE, 2010).

Em 16 de novembro de 2011, a SUBTEL, a agência reguladora do Chile, publica o resultado da inspeção que realizou em cada ISP no país, para verificar o cumprimento das obrigações estabelecidas na Lei. O resultado mostrou que existem ISPs que não facilitam o acesso dos consumidores à informação necessária, de forma transparente, destacada e clara. Para corrigir esta deficiência, a SUBTEL padronizou as informações mínimas exigidas pela Lei da Neutralidade, que devem ser fornecidas pelos ISPs, sob pena de multa em caso de descumprimento: (i) o nome e preço do plano; (ii) a velocidade publicitada em cada plano deverá conter uma velocidade máxima e uma velocidade mínima e, ainda, a velocidade de *download* e *upload*, indicando inclusive se há diferenças de acesso nacional e internacional; (iii) para tecnologias sem fio ou redes móveis, a oferta dos serviços deve expressar claramente que as faixas de velocidade estão sujeitas à variabilidade e comportamento probabilístico de acesso à Internet sem fio. Isto é inerente a este tipo de tecnologia e, por isso, deve conter as seguintes informações: mapas de cobertura por tipo de tecnologia, propagação do sinal, velocidades médias esperadas e toda a informação que permita um conhecimento profundo dos usuários, quando optarem por tais serviços; (iv) a chamada taxa de agregação deve especificar explicitamente a taxa de revenda de serviços de Internet. Esta taxa corresponde ao quociente entre a soma das velocidades contratadas por todos os usuários e a capacidade real contratada em Mbps no enlace, conforme o caso; e (v) limites de *download* (SUBTEL, 2011). Em 27 de maio de 2014 a SUBTEL, também com base na Lei da Neutralidade, oficiou os ISPs para acabarem com as promoções das chamadas Redes Sociais Gratuitas (taxa zero), sob a pena de multa (SUBTEL, 2014).

3.5. COLÔMBIA

Em 16 de junho de 2011, o governo da Colômbia aprova a Lei 1.450 referente ao Plano Nacional de Desenvolvimento para os anos de 2010 a 2014. A Lei prevê em seu Art. 56, as seguintes regras para a Neutralidade da Internet, a serem seguidas pelos ISPs. (i) Não podem bloquear, interferir, discriminar ou restringir o direito de qualquer usuário da Internet de usar, enviar, receber ou oferecer qualquer conteúdo, aplicação ou serviço legal através da Internet. Os ISPs devem oferecer a cada usuário um serviço de acesso à Internet ou conectividade, não distinguindo arbitrariamente conteúdos, aplicações ou serviços, com base na origem ou propriedade destes. Os ISPs podem fazer ofertas para as necessidades de segmentos específicos de mercado ou de seus usuários, de acordo com seus perfis de uso e de consumo, que não sejam interpretadas como discriminação. (ii) Não podem limitar o direito de um usuário usar qualquer tipo de instrumentos, ou dispositivos na rede, desde que sejam legais e que não danifiquem ou prejudiquem a qualidade da rede ou do serviço. (iii) Oferecerão aos usuários serviços de controle parental para conteúdos que atentem contra a Lei, prestando aos usuários informações antecipadas, de maneira clara e precisa a respeito do alcance de tais serviços. (iv) Publicarão em um *site*, toda a informação relativa às características do acesso à Internet oferecido, sua velocidade e qualidade do serviço, diferenciando entre as conexões nacionais e internacionais, assim como a natureza e garantias do serviço. (v) Implementarão mecanismos para preservar a privacidade dos usuários, contra vírus e a segurança da rede. Além disso, (vi) bloquearão o acesso a determinados conteúdos, aplicativos ou serviços, somente a pedido expresso do usuário (COLÔMBIA, 2011a).

A Resolução 3.502, de 16 de dezembro de 2011, estabelece as condições regulatórias relativas aos princípios da Neutralidade da Internet, em cumprimento ao estabelecido no artigo 56 da Lei 1.450 de 2011, conforme segue. (i) *Livre escolha*: o usuário é livre para usar, enviar, receber ou oferecer qualquer conteúdo, aplicativo ou serviço através da Internet, exceto nos casos em que por Lei ou ordem judicial estiverem proibidos, ou o seu uso estiver restrito. (ii) *Sem discriminação*: os ISPs devem sempre proporcionar igualdade de tratamento para o conteúdo, aplicações e serviços, sem qualquer discriminação arbitrária, especialmente na origem ou propriedade dos mesmos. (iii) *Transparência*: os ISPs devem divulgar suas políticas de gerenciamento

de tráfego aos usuários e outros provedores que tenham acesso à sua rede. (iv) *Informação*: os ISPs devem fornecer ao usuário toda a informação associada às condições de prestação do serviço, incluindo a velocidade, a qualidade, e as práticas de gerenciamento de tráfego relativas a cada plano oferecido ou acordado.

A Resolução 3.502, de 16 de dezembro de 2011, também estabelece os aspectos técnicos da Neutralidade da Internet na Colômbia, conforme segue. (i) Indicadores de qualidade do serviço de acesso à Internet. Os ISPs devem garantir em todo momento que as velocidades efetivas oferecidas sejam cumpridas, de acordo com as condições do plano. (ii) Bloqueio de conteúdos. Os ISPs não podem bloquear, interferir, discriminar, nem restringir o direito do usuário de usar, enviar, receber ou oferecer qualquer conteúdo, aplicação ou serviço através da Internet, sem o consentimento expresso do usuário. (iii) Segurança da rede. Os ISPs devem informar ao usuário, a qualquer momento, antes da celebração do contrato e durante a sua execução, os riscos relativos com a segurança da rede em termos do serviço contratado de acesso à Internet e as ações que devem ser antecipadas ao usuário para preservar a segurança da rede. (iv) Práticas de gerenciamento de tráfego. Os ISPs podem aplicar medidas de gerenciamento de tráfego que sejam razoáveis e não discriminatórias, a qualquer provedor, serviço, conteúdo ou protocolo.

De acordo com a mesma Resolução 3.502, as práticas de gerenciamento de tráfego são consideradas razoáveis quando elas se destinam a: (a) reduzir ou mitigar os efeitos do congestionamento na rede; (b) garantir a segurança e integridade das redes; (c) garantir a qualidade do serviço aos usuários; (d) priorizar tipos ou classes genéricas de tráfego em função dos requisitos de qualidade do serviço próprias deste tráfego, tais como latência e atraso dos mesmos; e (e) prestar serviços ou recursos de acordo com a escolha dos usuários, que atendam aos requisitos técnicos, normas ou melhores práticas adotadas por iniciativas de governança da Internet ou organizações de normatização; e (v) priorização de tráfego. Os ISPs não podem executar priorização, degradação ou bloqueio em violação às disposições desta resolução. Esta Resolução, ainda estabelece as condições regulatórias relativas à informação aos usuários, determinando o que deve constar dos planos e contratos ofertados pelos ISPs (COLÔMBIA, 2011b).

3.6. CORÉIA

A agência de regulação da Coréia do Sul, a KCC (*Korea Communications Commission*) traz, em seu relatório anual de 2011, um quadro contendo os Princípios Básicos para a Administração da Neutralidade da Rede e do Tráfego da Internet neste país. Os princípios são os seguintes. (i) Direitos do usuário: os usuários da Internet têm direito à informação sobre seu tráfego na Internet, sendo permitido livremente utilizar conteúdos legítimos, aplicações, e dispositivos, a menos que eles causem perigo (*hazard*) para os serviços ou redes. (ii) Administração transparente do tráfego da Internet. Os ISPs devem divulgar a finalidade, o escopo, as condições, os procedimentos e os métodos para administrar o tráfego da rede e devem também notificar os usuários dos detalhes ou efeitos das ações tomadas como necessárias para administrar o tráfego da rede. (iii) Proibição de bloqueio: quaisquer conteúdos, aplicações, aparelhos, ou dispositivos legítimos, não devem ser bloqueados, a menos que eles causem perigo para os serviços ou para as redes. (iv) Proibição de discriminação "não razoável" dos conteúdos, aplicações e serviços legítimos. (v) Gestão "razoável" do tráfego: o tráfego pode ser gerenciado, se necessário, para garantir a segurança e a proteção da rede, para eliminar a sobrecarga temporária ou o congestionamento da rede, ou conforme os estatutos pertinentes (KCC, 2012).

3.7. NOVA ZELÂNDIA

Em junho de 2011, a Comissão de Comércio, ente regulador das telecomunicações da Nova Zelândia, o ComCom (*Commerce Commission of New Zealand*), inicia um estudo para identificar quaisquer fatores que possam afetar os serviços de banda larga de alta velocidade na Nova Zelândia (COMCOM, 2012). Em 19 de dezembro de 2011, o ComCom publica o primeiro resultado do estudo, com quatro questões técnicas que identificou como relevantes para serviços de banda larga de alta velocidade: (i) os custos de instalações e o fornecimento de equipamento aos clientes; (ii) diferenciação de trânsito nacional e internacional; (iii) aspectos referentes a p*eering* e interconexões, além de Neutralidade da Rede; e (iv) barreiras que limitam o uso de dados (*data caps*) (COMCOM, 2011). Em 29 de junho de 2012, o ComCom publica o relatório final do estudo, no qual ressalta que a Neutralidade da Rede não deve ser um problema se os ISPs forem transparentes sobre as limitações ou as restrições impostas em seus serviços de banda larga. Ressalta também que o mercado dos ISPs é

suficientemente competitivo, e que os consumidores são capazes de mudar de ISPs, de forma relativamente fácil, se as restrições forem um problema. E ressalta ainda, que a Comissão é de opinião que a prática de taxa zero de determinados conteúdos, como por exemplo, o uso de *caches* de rede, é benéfico para os usuários finais. A Comissão espera que as pressões competitivas do mercado levem a barreiras mais elevadas de dados e na quantidade de conteúdo que é armazenado em *cache*; consequentemente, a prática e a importância do tráfego de taxa zero ficam suscetíveis de serem reduzidas (COMCOM, 2012).

Em 18 de junho de 2015 o *site* Internet NZ lança um documento de Discussão Pública (O'NEILL, 2015; NETWORK..., 2015), para buscar a opinião dos neozelandeses e iniciar um diálogo nacional, aberto e colaborativo, sobre o que Neutralidade da Rede significa na Nova Zelândia (INTERNETNZ..., 2015). Em 08 de setembro de 2015, o Ministério dos Negócios, Inovação e Emprego *(Ministry of Business, Innovation & Employment*) divulga um documento de discussão contínua e pública para revisão da Lei das Telecomunicações de 2001. Este documento também buscou angariar pontos de vista sobre uma série de opções para a regulação das comunicações após o ano de 2020, encorajando as partes interessadas, as empresas e os consumidores a participar. Para isto, levanta várias questões, sendo que algumas delas referem-se de forma direta à Neutralidade da Rede conforme segue. (i) Há questões atuais de Neutralidade da Rede na Nova Zelândia? (ii) O regime regulador é capaz de abordar as questões da Neutralidade de Rede se elas surgirem na Nova Zelândia? Se não, qual abordagem deve ser considerada? (iii) Há gerenciamento de tráfego aceitável e não aceitável? Por favor, forneça exemplos específicos e realistas. Por exemplo, os ISPs devem: (a) ser capazes de bloquear ou não priorizar (*deprioritise)* conteúdos legais, aplicações ou serviços? (b) ser capazes de entrar em acordos comerciais com provedores de conteúdo para priorizar determinado tráfego? e (c) ser capazes de priorizar certos tipos de tráfego, quando a rede está congestionada (como tráfego de voz ou serviços de chamadas de emergência)? e (iv) existem outras questões sobre a Neutralidade da Rede que devam ser consideradas no contexto de uma regulamentação (por exemplo, práticas de distribuição de conteúdo)? (NOVA ZELÂNDIA, 2015). Todas as contribuições recebidas estão disponíveis na página do Ministério (NOVA ZELÂNDIA, [2001]).

Embora tenham sido encontradas várias considerações sobre a Neutralidade da Rede na Nova Zelândia, e algumas questões inerentes tenham sido postas em consulta

pública, até o final desta pesquisa nenhum tipo de normatização foi encontrada, levando a crer que o assunto permanece em discussão neste país.

3.8. RÚSSIA

Em 11 de fevereiro de 2014, o governo da Federação Russa aprovou o plano de ação para o desenvolvimento da concorrência no setor das telecomunicações, elaborado pelo Ministério das Comunicações, com a participação do FAS, o Serviço Federal Antimonopólio (*Federal Antimonopoly Service*). Segundo o FAS, neste plano de ação foram incluídas medidas destinadas a apoiar a Neutralidade da Rede. (FAS, 2014). Ao executar o plano de ação, o FAS elaborou um relatório sobre a aplicação dos princípios da Neutralidade da Rede em redes de telecomunicações, propondo formalizar as disposições que determinam a política de Neutralidade, nos seguintes atos normativos legais: a Lei federal sobre as comunicações, as regras para a conexão de redes de telecomunicações, além de regras para os serviços de comunicações. As consultas públicas sobre estes atos normativos legais para formalizar os princípios da Neutralidade da Rede começaram em 12 de novembro de 2014 e em 27 de janeiro de 2015. O FAS participou de uma audiência pública com representantes do setor das telecomunicações e da Tecnologia da Informação e Comunicação. Como resultado desta audiência pública, os especialistas chegaram à conclusão que as normas gerais da Lei antimonopólio abrangem os principais princípios da Neutralidade da Rede. E, foi tomada a decisão de estabelecer um Grupo de Trabalho do FAS para a aplicação dos princípios da Neutralidade da Rede na Federação Russa, com o envolvimento dos reguladores e do mercado (FAS, 2015a).

Em 20 de abril de 2015, este Grupo de Trabalho teve sua primeira reunião, e como nenhum fato de violação dos princípios da Neutralidade da Rede foi revelado, também concluiu que o cumprimento das normas gerais da Lei antimonopólio apoia os princípios da Neutralidade da Rede (FAS, 2015c). A segunda reunião do Grupo de Trabalho ocorreu em 30 de Novembro de 2015, e nela os participantes acordaram em empregar uma regulação "cuidadosa" sobre a Neutralidade da Rede, cuja finalidade é apoiar o desenvolvimento da Internet como uma plataforma aberta para inovações, diminuindo barreiras de acesso para usuários finais, operadores e fornecedores de conteúdo e serviços (FAS, 2015b). Em 16 de Dezembro de 2015 houve a terceira

reunião do Grupo. Esta reunião ocorreu para discutir os objetivos, conceitos e princípios fundamentais da Neutralidade da Rede, descritos em um projeto sobre a Neutralidade da Rede a ser refinado na próxima reunião (FAS, 2015d).

Em 23 de fevereiro de 2016 o Grupo de Trabalho elaborou um documento que chamou de "Documento Fundamental sobre a Neutralidade da Rede". Este documento teve como finalidade assegurar o acesso não discriminatório, e as condições de desempenho para os provedores de serviços e de conteúdo. Além disso, o documento teve como finalidade criar condições para o desenvolvimento das telecomunicações, da concorrência e de uma cooperação entre os participantes do mercado, considerando que estas condições certamente irão facilitar os investimentos e as inovações. Todos os membros do Grupo de Trabalho, representantes do Ministério das Comunicações, especialistas do governo, especialistas independentes, e representantes da indústria de comunicações e da comunidade da tecnologia de informação e comunicação, concordaram em observar os princípios da Neutralidade da Rede (FAS, 2016).

Ainda que tenham sido encontradas no *site* do FAS as menções aos documentos acima citados, elaborados pelo Grupo de Trabalho em defesa e adoção dos princípios da Neutralidade da Rede, nenhum destes documentos foi localizado no *site*. Ou seja, não foi encontrado qualquer tipo de documento que contenha a normatização propriamente dita, que liste os princípios ou regras a serem adotados pelos ISPs.

3.9. BRASIL

No Brasil, embora a normatização da Neutralidade da Rede comece a se concretizar somente em 2014, desde 2007 ocorriam discussões em torno da necessidade de regulamentar a Internet, chegando a tramitar um Projeto de Lei de crimes virtuais que propunha que o primeiro marco regulatório da Internet brasileira fosse criminal (LEMOS, 2007). Entretanto, o governo brasileiro decidiu por um marco civil em vez de um marco criminal e, a partir de 2009, são tomadas as primeiras providências para a construção deste marco civil. Em 05 de junho de 2009, o CGI.br (Comitê Gestor da Internet no Brasil), ente responsável pela governança da Internet no Brasil, aprova e lança uma Resolução com os 10 Princípios para a Governança e Uso da Internet no Brasil (CGI, 2009b), na qual, a Neutralidade da Rede, aparece como o sexto princípio (CGI, 2009a). Em 29 de outubro de 2009, a Secretaria de Assuntos Legislativos do

Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro, da Fundação Getúlio Vargas, lança o projeto para a construção colaborativa do Marco Civil, tomando como base os 10 princípios estabelecidos pelo CGI.br. O processo para esta construção colaborativa ocorreu em duas fases e todo o código da consulta pública foi disponibilizado sob licença AGPL 3.

Na primeira fase, foram debatidas ideias sobre os tópicos propostos para a regulação, a partir de um texto-base produzido pelo Ministério da Justiça, contendo ideias, princípios e valores. Na segunda fase, a discussão teve como parâmetro a minuta do Anteprojeto de Lei do Marco Civil. Cada artigo, parágrafo, inciso ou alínea deste Anteprojeto de Lei, também esteve aberto para participação da sociedade, em forma de consulta pública. Também ocorreram foros de discussão para o amadurecimento de ideias e para uma discussão irrestrita (BRASIL, [2016a]). Estas duas fases resultaram na elaboração do Projeto de Lei, PL 2.126, de 2011, que estabeleceu os princípios, as garantias, os direitos e os deveres para o uso da Internet no Brasil e que, em 24 de agosto de 2011, foi encaminhado ao Congresso Nacional pela então presidente do Brasil, Dilma Rousseff, para apreciação (BRASIL, 2011b). Em 25 de março de 2014, a Câmara dos Deputados aprova este Projeto de Lei, em 26 de março de 2014 o encaminha ao Senado Federal e, em 23 de abril de 2014, ele é transformado na Lei Ordinária 12.965 (BRASIL, 2011a).

A Neutralidade da Rede está exposta no Artigo 9º da Lei Ordinária 12.965, determinando que o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação. Salienta que: (i) a discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República, para a fiel execução desta Lei. Para isto, serão ouvidos o CGI.br e a Anatel (Agência Nacional de Telecomunicações). A discriminação ou degradação do tráfego, somente poderá decorrer de requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações. A priorização, somente é permitida para os serviços de emergência. (ii) Na hipótese de discriminação ou degradação do tráfego prevista, o ISP deve abster-se de causar dano aos usuários. Deve agir com proporcionalidade, com transparência e com isonomia. Deve informar previamente, de modo transparente, claro e suficientemente descritivo aos seus usuários, quais as práticas adotadas para o gerenciamento e a mitigação de tráfego, inclusive as relacionadas à segurança da rede. Deve oferecer serviços em condições comerciais não

discriminatórias e, ainda, deve abster-se de praticar condutas anticoncorrenciais. Além disso, (iii) na provisão de conexão à Internet, paga ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado ao ISP bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados (BRASIL, 2014).

Assim, em atendimento ao exposto na Lei do Marco Civil, para poder fornecer as informações devidas à Presidente da República quanto a discriminação ou degradação do tráfego, o CGI.br realizou uma consulta pública entre 19 dezembro de 2014 e 20 de fevereiro de 2015, para recolher os subsídios da sociedade (CGI, 2015). O Ministério da Justiça também promoveu sua consulta pública, entre 28 de janeiro e 30 de abril de 2015 e, por meio dela, recebeu mais de 60 mil visitas e cerca de 1.200 comentários da população (BRASIL, [2016a]). E, da mesma forma, a Anatel realizou a sua consulta pública entre os dias 31 de março e 19 de maio de 2015, com o objetivo de colher da sociedade os elementos para subsidiar a sua participação na regulamentação, junto à Presidência da República (ANATEL, 2015c). Em 10 de novembro de 2015, o CGI.br encaminha ao Ministério da Justiça e à Casa Civil, o documento elaborado a partir das contribuições recebidas em sua consulta pública, e das contribuições vindas a partir de discussões ocorridas no âmbito de um grupo de trabalho, especificamente constituído para tratar da regulamentação (CGI, 2015).

Como resultado das contribuições recebidas, o Ministério da Justiça elabora a minuta do Decreto Presidencial para regulamentar o Marco Civil (BRASIL, [2016b]) e, em 27 de janeiro de 2016, a apresenta à sociedade em nova Consulta Pública, para que os interessados pudessem dar contribuições e sugerir alterações de redação ou de conteúdo, até o dia 29 de fevereiro (BRASIL, [2016b]). Em 28 de janeiro de 2016 a Abranet, a Associação Brasileira de Internet, publica uma crítica a esta minuta de Decreto, destacando que ela é bastante genérica em relação à taxa zero e às exceções à Neutralidade da Rede (PRESCOTT, 2016).

Em 18 de abril de 2016 (COSTA, 2016), o presidente do órgão regulador do Brasil, a Anatel, afirma que “a era da Internet ilimitada acabou”. Pode-se compreender que para a Anatel as operadoras de banda larga fixa devem descontinuar os serviços sem limitação, o que obrigará o segmento a migrar para o modelo de franquias, semelhante aos serviços de Internet móvel. Em 20 de abril de 2016, o CGI.br deliberou pela criação de um grupo de trabalho para debater e estabelecer posicionamento sobre o tema da franquia de dados na banda larga fixa, até 20 de maio de 2016 (CGI, 2016a). Em consequência, em 3 de maio de 2016, houve uma audiência pública para discutir este

tema da franquia de dados na banda larga fixa (ANATEL..., 2016), presidida pelo senador Lasier Martins (PDT-RS), no Congresso Nacional. Participaram desta audiência pública o presidente do Conselho Federal da Ordem dos Advogados do Brasil, Claudio Lamachia, o presidente do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), Demi Getschko, além de representantes das empresas prestadoras de serviço. Também foram convidados os ministérios das Comunicações e da Justiça, a Anatel, o Ministério Público, o Instituto Brasileiro de Defesa do Consumidor (Idec) e a Proteste (Associação Brasileira de Defesa do Consumidor), entre outros.

Nesta audiência pública, o presidente do Conselho Federal da Ordem dos Advogados do Brasil, Claudio Lamachia, solicitou ao Senado a tomada de providências quanto à polêmica sobre a Anatel, criticando o posicionamento de seu presidente, que havia sugerido que a era da Internet ilimitada chegou ao fim, e da possibilidade de limitar o uso de dados por consumidores de Internet banda larga. Lamachia afirma que é preciso avaliar o papel que vem sendo desempenhado pela Anatel, visto que "ela deve atuar na defesa do consumidor, e não como um sindicato das empresas de telefonia". Segundo Lamachia, "a Anatel tem compromissos com a sociedade e a função de regular o mercado", enfatizando que é preciso examinar o papel que a Anatel vem cumprindo no Brasil e qual é a real finalidade desta agência reguladora. Lamachia também esclareceu que a limitação do uso de dados na Internet fere diretamente o Código de Defesa do Consumidor e o Marco Civil da Internet. O conselheiro da Anatel, Rodrigo Zerbone, por sua vez, explicou na mesma audiência pública, que a Anatel decidiu, após ser oficiada pela OAB, reanalisar a cautelar que regulamentou o uso de franquias. Também informou que deveria ser criado grupo de trabalho com todos os atores envolvidos na discussão para ajudar o conselho diretor da agência (ANATEL..., 2016).

Em 05 de maio de 2016 a presidente Dilma Rousseff recebe do Ministério da Justiça a minuta do Decreto que vai regulamentar o Marco Civil da Internet. Este texto proíbe os ISPs de ofertar pacotes de taxa zero, que não descontam o tráfego de alguns aplicativos das franquias contratadas, e que comprometem o caráter público e irrestrito do acesso à Internet (GROSSMANN; QUEIROZ, 2016). Por fim, em 11 de maio de 2016, a presidente Dilma Rousseff assina o Decreto 8.771 que regulamenta a Lei 12.965, de 23 de abril de 2014. Este Decreto trata das hipóteses admitidas de discriminação de pacotes de dados na Internet, e de degradação de tráfego. O Decreto também indica os procedimentos para a guarda e a proteção de dados por provedores de conexão e de aplicações. E, ainda, este Decreto também aponta as medidas de

transparência na requisição de dados cadastrais pela administração pública e estabelece os parâmetros para a fiscalização e a apuração de infrações. De maneira específica, o texto do Decreto 8.771 deixa claro que ele não se aplica: (i) aos serviços de telecomunicações que não se destinem ao provimento de conexão de Internet; e (ii) aos serviços especializados, desde que: (a) não configurem substituto à Internet em seu caráter público e irrestrito; e (b) sejam destinados a grupos específicos de usuários com controle estrito de admissão (BRASIL, 2016a).

Do mesmo modo, o Decreto 8.771 deixa claro que reitera o exposto no art. 9º da Lei nº 12.965, de 2014, garantindo a preservação do caráter público e irrestrito do acesso à Internet; e enfatizando que a discriminação ou a degradação de tráfego são medidas excepcionais, na medida em que somente poderão decorrer de requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações, ou da priorização de serviços de emergência. Além disso, o Decreto 8.771 elucida que ficam vedadas as condutas unilaterais ou os acordos entre o responsável pela transmissão, pela comutação ou pelo roteamento e os provedores de aplicação que: (i) comprometam o caráter público e irrestrito do acesso à Internet e os fundamentos, os princípios e os objetivos do uso da Internet no País; (ii) priorizem pacotes de dados em razão de arranjos comerciais; ou (iii) privilegiem aplicações ofertadas pelo próprio responsável pela transmissão, pela comutação ou pelo roteamento ou por empresas integrantes de seu grupo econômico. E, ainda, o Decreto 8.771 ressalta que as ofertas comerciais e os modelos de cobrança de acesso à Internet devem preservar uma Internet única, de natureza aberta, plural e diversa, compreendida como um meio para a promoção do desenvolvimento humano, econômico, social e cultural, contribuindo para a construção de uma sociedade inclusiva e não discriminatória (BRASIL, 2016a).

Dentre outros aspectos, o Decreto regulamenta a Neutralidade da Rede no Brasil e proíbe a prática de taxa zero, embora de forma implícita, considerando que o termo não é empregado no seu texto. Também sobre esta prática, em 11 de novembro de 2015, foi divulgada a Nota Técnica Nº 02/2015, do Ministério Público Federal, que analisou o Projeto Internet.org do Facebook e o princípio da Neutralidade da Rede. O Projeto Internet.org refere-se ao serviço *Freebasics*, considerado como taxa zero. De acordo com o Ministério Público Federal, o Projeto Internet.org, ou *Freebasics*, é um aplicativo que permite o acesso limitado a determinadas aplicações e conteúdos previamente aprovados pelo Facebook, violando os princípios norteadores da Internet no Brasil, o

princípio da Neutralidade da Rede e a Internet livre, preconizados no Marco Civil brasileiro (BRASIL, [2015]).

Em 16 de agosto de 2016, o responsável pela Secretaria Nacional do Consumidor (Senacon), Armando Luiz Rovai, informa que a Senacon instalou um grupo de trabalho dentro do Departamento de Proteção e Defesa do Consumidor (DPDC) (AMARAL, 2016). A criação deste grupo de trabalho visa monitorar a Internet para prevenir abusos, funcionando de maneira preventiva, para evitar que o consumidor seja lesado. Isso ocorreu em atendimento à atribuição recebida pela Senacon no Decreto nº 8.711/2016 de maio, que regulamenta o Marco Civil, de reger a Neutralidade da Rede, em conjunto com a Anatel e com o Conselho Administrativo de Defesa Econômica (Cade). Rovai também frisou o papel do CGI.br neste mesmo decreto, que o torna responsável por estabelecer as diretrizes, que devem ser seguidas pela Anatel, nos casos da regulação das exceções para o gerenciamento e a degradação do tráfego da rede. Rovai ainda enfatiza a importância de uma relação sinérgica entre a Senacon, o CGI.br e a Anatel para poderem cumprir com o exposto no referido decreto.

Em 11 de novembro de 2016 a Anatel deu início ao processo de consulta pública sobre as franquias de dados na banda larga fixa (ANATEL, 2016). A Anatel esclarece que as contribuições recebidas em resposta a esta consulta pública, somar-se-ão a outras formas de participação da sociedade nesse processo regulatório, por meio de debates públicos e audiências públicas. Todos os subsídios colhidos junto à sociedade no decorrer das etapas serão considerados na sistematização destinada a instruir o processo decisório. A Anatel salienta que, enquanto a decisão final não for tomada, as operadoras de banda larga fixa continuam proibidas de reduzir a velocidade, suspender o serviço ou cobrar pelo tráfego excedente nos casos em que os consumidores utilizarem toda a franquia contratada (quando houver), ainda que tais ações estejam previstas em contrato de adesão ou plano de serviço, nos termos de decisão tomada pelo Conselho Diretor da Anatel.

A associação de consumidores sem fins lucrativos, chamada PROTESTE, se manifestou nesta consulta pública da Anatel. Sua manifestação foi contra a aplicação da franquia nos planos de acesso a banda larga (PROTESTE, 2016), seja pela rede móvel, seja pela rede fixa. Na avaliação da PROTESTE, o Marco Civil da Internet não introduziu essa diferença, e tampouco o Código de Defesa do Consumidor.

Para a PROTESTE, o consumidor não tem como controlar o consumo de sua franquia, pois faltam mecanismos de informação sobre a utilização dos dados. Esta

Associação entende que a franquia cria uma situação de vantagem injustificada para empresas que já concentram fatia substancial do setor. A PROTESTE entende também que não cabe à Anatel, de forma exclusiva, editar normas que autorizem ou desautorizem os planos de franquia de dados, seja no que diz respeito aos acessos à Internet pela rede móvel, seja pela rede fixa. Especialmente porque o Marco Civil da Internet estabeleceu a governança multisetorial com participação do CGI.br.

A PROTESTE entrou com ação civil pública, no Tribunal de Justiça de São Paulo, para impedir que as operadoras Vivo, Oi, Claro, TIM, e NET vendam novos planos, com previsão de bloqueio à conexão após fim da franquia em redes celulares 3G e na Internet fixa. Caso tenha sucesso, a medida valerá para todo o País. No entender desta Associação, o bloqueio do acesso à Internet ao consumidor que pagou pelo acesso, fere não só o direito à continuidade do serviço de interesse público, mas também o princípio da neutralidade, ambos constantes no Marco Civil da Internet (PROTESTE, 2016).

Em 23 de novembro de 2016, o secretário de políticas de informática do MCTIC, e que também exerce a coordenação do (CGI.br), Maximiliano Martinhão afirma, no evento Painel Telebrasil 2016 (GROSSMANN; COSTA, 2016), que "não é possível pensar com tamanha rigidez a Neutralidade de Rede", se referindo a serviços como a taxa zero. Segundo ele, "para que se possa avançar com a Internet é preciso exercer flexibilidade". Porque, segundo ele, "quando essas questões foram pensadas no Marco Civil, se pensava muito no usuário final. Isto gera insegurança grande, e por isto deve haver ajustes no decreto regulamentador do Marco Civil da Internet ou na lei de proteção de dados pessoais em trâmite no Congresso Nacional".

Em 20 de dezembro de 2016, o texto do Projeto de Lei, PLC 79/2016 (BRASIL, 2016b), que altera a Lei Geral das Telecomunicações, foi aprovado na Câmara dos Deputados. Este Projeto de Lei, chamado pela mídia de "escândalo da teles", conta com o apoio do Ministério das Comunicações, do então Ministro Gilberto Kassab. Caso este Projeto de Lei seja aprovado em todas as instâncias, e na forma como se apresenta, ele poderá repassar às empresas de telefonia que atuam no Brasil, mais de 80 bilhões de reais em patrimônio de infraestrutura de rede instalada, como também poderá perdoar dívidas destas empresas, estimadas em 20 bilhões de reais (GOVERNO..., 2016). Este Projeto de Lei encontra-se no Senado Federal. Todos os projetos de lei e demais proposições que tramitam no Senado ficam abertos para receber opiniões desde o início até o final de sua tramitação. A consulta pública para o PLC 79/2016 encerrou em

março de 2017, obtendo 695 votos contra e 23 votos favoráveis a sua aprovação (BRASIL, 2016c).

Em 13 de janeiro de 2017, há um retorno à mídia sobre a questão do limite de dados na banda larga fixa. Em entrevista (KLEINA, 2017), o ministro Gilberto Kassab afirma que haverá regulamentação da venda de pacote de dados, de banda larga fixa, para o segundo semestre de 2017, acabando assim, com a oferta de Internet ilimitada na rede fixa. O ministro argumenta que a prática será benéfica para o setor de telecomunicações e que o objetivo "é beneficiar o usuário". De acordo com Kassab, "haverá um período de adaptação no qual os assinantes terão certos limites em seus pacotes de consumo, e poderá haver alteração na cobrança, por parte da operadora". Para o ministro, "a ideia é que esse serviço seja o mais elástico possível, mas tenha um ponto de equilíbrio, visto que as operadoras têm seus limites".

Em 13 de janeiro de 2017, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) publica em seu *site* uma nota de esclarecimento. Nesta nota o Ministro Gilberto Kassab muda completamente o seu posicionamento e esclarece que "não haverá mudanças no modelo atual de planos de banda larga fixa, reiterando seu compromisso em atender o interesse da população e do consumidor" (BRASIL, 2017b).

Em 14 de março de 2017, O Instituto Brasileiro de Defesa do Consumidor (Idec) reitera sua posição sobre o PLC 79. A visão desta organização (IDEC..., 2017), subscrita por outras organizações sociais participantes da Coalizão Direitos na Rede, é que "o PLC 79 dá muito poder à Anatel e ao Executivo, enquanto elimina os compromissos das concessionárias com a universalização de serviços". Para Rafael Zanatta, pesquisador do Idec, "deixar a regulamentação das obrigações somente com o governo, vai contra a arquitetura de governança do uso e expansão da Internet no Brasil, definido pelo Marco Civil da Internet. Se os compromissos de investimento servem à inclusão digital e redução de desigualdades, então a lógica a se seguir não é somente a da Lei Geral de Telecomunicações, como o que está sendo proposto pelo PLC 79, mas também a sistemática criada pelo Marco Civil da Internet" (IDEC..., 2017).

Em 15 de março de 2017, o plenário do Senado Federal aprovou o projeto PLS 174/2016, do senador Ricardo Ferraço, que proíbe as operadoras de Internet de estabelecer franquias de dados em seus contratos de banda larga fixa. Este projeto altera a Lei 12.965/2014, do Marco Civil da Internet, para vedar, expressamente, os planos de franquias de dados para esse tipo de serviço (BRASIL, 2017c). O PLS 174/2016 não

altera as regras dos planos de Internet móvel e, em 21 de março de 2017, foi remetido à Câmara dos Deputados para análise (BRASIL, 2017a).

3.10. MÉXICO

Em 14 de julho de 2014, o governo mexicano altera sua Lei Federal de Telecomunicações e Radiodifusão (MÉXICO, 2014), incluindo dois itens específicos para a Neutralidade da Rede: (i) os ISPs, que prestam serviços de acesso à Internet, deverão sujeitar-se às orientações gerais emitidas pelo Instituto Federal de Telecomunicações, como segue. (a) A liberdade de escolha deve ser assegurada, os usuários dos serviços de acesso à Internet terão acesso a qualquer conteúdo, aplicação ou serviço ofertado, dentro do quadro legal aplicável, sem limitar, degradar, discriminar ou restringir o acesso aos mesmos. (b) Os ISPs, autorizados a comercializar o serviço de fornecimento de acesso à Internet, terão que se abster de obstruir, interferir, inspecionar, filtrar ou discriminar conteúdos, aplicações ou serviços. (c) A privacidade deve ser assegurada. Os ISPs deverão preservar a privacidade dos usuários e a segurança da rede. (d) A transparência e a informação devem ser asseguradas. Os ISPs deverão publicar na sua página da Internet informações relativas às características do serviço ofertado. Isto inclui as políticas de gerenciamento de tráfego autorizadas pelo Instituto, a velocidade, a qualidade, a natureza e a garantia do serviço. (e) Finalmente, trata do gerenciamento de tráfego, descrita a seguir.

Os ISPs poderão tomar as medidas ou ações necessárias para o gerenciamento do tráfego conforme as políticas autorizadas pelo Instituto, a fim de garantir a qualidade ou a velocidade do serviço contratado pelo usuário, desde que isto não constitua uma prática contrária à competição saudável e a livre concorrência. (f) A qualidade deve ser assegurada, os ISPs deverão manter os padrões mínimos de qualidade previstos nas diretrizes correspondentes. (g) O desenvolvimento sustentável da infraestrutura deve ser garantido. Nas diretrizes correspondentes, o Instituto deverá promover o crescimento sustentável da infraestrutura de telecomunicações.

O segundo item sobre a Neutralidade da Rede tratado na Lei Federal determina que os ISPs deverão fornecer o serviço de acesso à Internet respeitando a capacidade, a velocidade e a qualidade contratada pelo usuário, independentemente do conteúdo, da

origem, do destino, ou da aplicação, bem como deverão fornecer os serviços prestados através da Internet, em cumprimento ao estabelecido no item anterior.

3.11. ESTADOS UNIDOS

Nos Estados Unidos, as regras para garantir uma Internet aberta foram adotadas pela FCC *(Federal Communications Commission)* em 26 de fevereiro de 2015. Entretanto, desde 2002 a FCC vinha tomando várias medidas para que isto ocorresse, conforme já exposto nesta tese no item 1.1. Em 08 de fevereiro de 2004, Michael K. Powell, então Presidente da FCC, proferiu palestra na Escola de Direito da Universidade do Colorado (*University of Colorado School of Law*) sobre a preservação da liberdade na Internet. Na palestra, destaca que os consumidores são os juízes finais na percepção se a indústria está preservando com sucesso a liberdade da Internet (POWELL, 2004). Em 5 de agosto de 2005, a FCC divulga que a Suprema Corte concordou com a sua posição adotada em 2002, que o serviço de fornecimento de acesso à Internet é um serviço de informação (ver item 1.1.) (FCC, 2005b). Também em 05 de Agosto de 2005, a FCC publica um *Policy Statement* sobre a Internet de banda larga, de acordo com as diretivas dadas pelo Congresso Americano, a fim de fomentar a criação, a adoção e o uso de conteúdo, aplicativos e serviços para garantir que os consumidores se beneficiem com a inovação que vem da concorrência (FCC, 2005a).

Em 16 de julho de 2007, a FCC finaliza a sua consulta pública sobre a Neutralidade da Rede, obtendo um total de 27.000 comentários a favor e contra, provenientes de empresas, consumidores e representantes do governo, sendo que a maioria dos participantes foi de usuários comuns da Internet que enviaram seus comentários por e-mail (ANDERSON, 2007). Em 12 de Fevereiro de 2008, o Congresso Americano, aprova a Lei HR 5.353 denominada Preservação da Liberdade na Internet (*Internet Freedom Preservation*) a fim de direcionar a FCC a conduzir um processo para avaliar a concorrência, a defesa do consumidor, e as questões relacionadas à liberdade de escolha do consumidor para serviços de acesso à Internet de banda larga (UNITED STATES OF AMERICA, 2008). Em 22 de outubro de 2009, a FCC lança uma proposta de regulamentação, e pede comentários ao público, sobre as práticas da indústria de banda larga, em especial sobre as regras para permitir aos provedores de banda larga administrar razoavelmente suas redes, e ajudar a garantir

uma Internet segura, onde o tráfego indesejado, tais como vírus de computador e *spam*, é limitado (FCC, 2009).

Em 21 de dezembro de 2010, a FCC adota três regras básicas para preservar a Internet como uma plataforma aberta para a inovação, o investimento, a criação de emprego, o crescimento econômico, a concorrência, e a livre expressão: (i) a transparência (*transparency*); (ii) nenhum bloqueio (*no blocking*), e (iii) nenhuma discriminação não razoável (*no unreasonable discrimination*) (FCC, 2010). Em 2 de agosto de 2011, a FCC efetua a primeira medição da banda larga nos Estados Unidos para verificar se os consumidores residenciais estavam recebendo desempenho próximo ao nível anunciado pelos seus provedores (FCC, 2012b). Aproximadamente um ano depois, o relatório de julho de 2012 revela as melhorias no serviço de banda larga residencial com impacto substancial sobre a indústria e sobre a experiência do consumidor de banda larga (FCC, 2012a). Estas melhorias no serviço ofertado pelos ISPs fazem com que a FCC mantenha as medições da banda larga nos Estados Unidos ano a ano, disponibilizando para isto um software de código aberto, e oferecendo resultados de testes de desempenho de banda larga para 13 dos maiores ISPs de rede fixa, que servem mais de 80 por cento do mercado residencial norte-americano (FCC, 2015a).

Em 14 de janeiro de 2014, as três regras adotadas pela FCC em 2010 são julgadas pela Corte de Apelação do Distrito de Columbia (*The United States Court of Appeals for the District of Columbia*). Como resultado do julgamento, esta Corte de Apelação afirma a autoridade da FCC para regular o serviço de acesso à Internet de banda larga, sanciona a regra da transparência, mas anula as regras de não bloqueio e de discriminação não razoável, por considerar que não são práticas ilícitas quando classificadas em "serviços de informação" *versus* "serviços de telecomunicações" (FCC, 2014b). Em 08 de maio de 2014, 122 investidores em tecnologia, como por exemplo, fundos de pensão, e instituições financeiras, enviam uma carta à FCC, encorajando a Comissão a considerar todas as ferramentas jurisdicionais disponíveis, no sentido de garantir uma Internet livre e aberta que recompense, sem prejuízo, o investimento e o empreendedorismo. Esta carta é uma crítica às regras da FCC. Segundo estes investidores, as regras não contemplam todos os pontos necessários para garantir a Neutralidade da Rede porque não impede, por exemplo, que os ISPs trafeguem o conteúdo na Internet por meio das chamadas "pistas rápidas e lentas" (priorização paga). Os investidores deixam claro à FCC nesta carta que precisam de regras simples,

fortes e exequíveis contra a discriminação e as taxas de acesso, e não apenas contra o bloqueio. (LETTER..., 2014*).* Em 15 de maio de 2014, a FCC lança nova consulta pública com o objetivo de encontrar a melhor abordagem para proteger e promover a Internet aberta, recebendo comentários até 15 de julho e respondendo-os até 10 de setembro de 2014 (FCC, 2014a).

Finalmente, nas regras adotadas em 26 de fevereiro de 2015 (FCC, 2015c), a FCC volta a classificar o acesso de banda larga à Internet como um "serviço de telecomunicações" o que lhe garante o fundamento jurídico necessário para preservar e proteger a Internet aberta. As regras adotadas visam proteger e manter o acesso aberto e livre para os conteúdos lícitos *online*, sem que os ISPs estejam autorizados a bloquear, prejudicar, ou estabelecer pistas rápidas e lentas para os conteúdos lícitos. De acordo com a FCC, estas novas regras foram projetadas para proteger a liberdade de expressão e inovação na Internet, e promover o investimento em redes de banda larga do país. Também para a FCC, estas novas regras foram fundamentadas na base legal mais forte possível, e aplicam-se aos serviços de banda larga fixa e móvel (FCC, 2015b).

Dentre as 400 páginas deste documento de normatização, denominado FCC 15-24 - *Report and Order on Remand, Declaratory Ruling, and Order*, de 26 de fevereiro de 2015, destacam-se pela sua inerência à Neutralidade da Rede, as seguintes regras que visam proteger os consumidores de táticas que ameaçam a Internet aberta, descritas a seguir: (i) Não bloqueio: os consumidores de Internet de banda larga devem obter o que pagaram, ou seja, ter acesso a todos os destinos (legais) na Internet. (ii) Não estrangulamento: a proibição de estrangulamento é necessária tanto para satisfazer as expectativas razoáveis de um cliente de banda larga de ter acesso a toda a Internet legítima, quanto para evitar alguma artimanha concebida para evitar a regra de não haver bloqueio. O não estrangulamento proíbe a degradação do tráfego da Internet com base na origem, destino ou conteúdo. Também proíbe especificamente a conduta que prioriza conteúdos específicos, por exemplo, que competem com serviços do próprio provedor de banda larga.

(iii) Não Priorização Paga: a priorização paga ocorre quando um ISP aceita pagamento (monetário ou não) para gerenciar sua rede de uma forma que beneficia determinado conteúdo, aplicação, serviço ou dispositivo. A priorização paga refere-se à gestão da rede de um ISP para favorecer direta ou indiretamente, algum tráfego sobre outros tipos de tráfego, incluindo uso de técnicas como a engenharia de tráfego, a priorização, a reserva de recursos, ou outras formas de gerenciamento de tráfego

preferencial, em troca de benefício monetário ou não, recebido de um terceiro, ou, para beneficiar uma entidade afiliada. (iv) Transparência: assegurar a transparência, para que os consumidores sejam plenamente informados sobre o acesso à Internet que estão pagando e para que os provedores de borda tenham a informação de que necessitam para compreender se os seus serviços irão funcionar como anunciado. (v) Interconexão: o Serviço de Acesso à Internet de banda larga – BIAS (*Broadband Internet Access Service*) envolve a troca de tráfego entre um ISP e as redes de conexão. Segundo esta regra, os clientes devem ser capazes de alcançar, "todos ou substancialmente todos os destinos de Internet", incluindo necessariamente, a promessa de fazer os acordos de interconexão necessários para permitir esse acesso (FCC, 2015c).

Quanto à taxa zero, a FCC salienta que tal prática tem o potencial de distorcer a concorrência, permitindo que os prestadores de serviços escolham entre conteúdo e aplicativos, ao mesmo tempo em que novas ofertas de serviços, dependendo de como elas sejam estruturadas, podem beneficiar os consumidores e a concorrência. Por conseguinte, a FCC decide analisar e avaliar tais práticas sob o padrão da interferência, da desvantagem, da não razoabilidade, com base nos fatos de cada caso individualmente e, após, isso, tomar as medidas necessárias (FCC, 2015c).

De acordo com Klint Finley, após a adoção das regras da Internet aberta, que teoricamente, inauguraram a era da Neutralidade da Rede, a batalha com as forças que se opõem a ela está longe de terminar, visto que existem ameaças vindas de várias direções (FINLEY, 2016). Desde a adoção das suas regras, a FCC vem sofrendo pressão dos opositores. Na moção de rejeição, de 08 de maio de 2015, junto ao tribunal de Apelações do Distrito de Colúmbia, a FCC cita petições que foram movidas por algumas organizações, contra as suas regras da Neutralidade da Rede, logo após serem instituídas, conforme segue. Em 23 de março de 2015 foram apresentadas petições pela *Alamo Broadband* e a *The United States Telecom Association* (*USTelecom*). Em 14 de abril de 2015, a *Alamo Broadband* novamente apresenta outro pedido de revisão das regras e, em 23 de abril de 2015, uma petição foi feita por um grupo que incluiu a *Full Service Network,* a *TruConnect Mobile*, a *Sage Telecommunications LLC,* e a *Telescape Communications* (UNITED STATES OF AMERICA, 2015).

Em 25 de fevereiro de 2016, o senador dos Estados Unidos, Mike Lee, propôs um projeto de Lei para proibir a FCC de reclassificar o serviço de acesso à Internet de banda larga como um serviço de telecomunicações, e de impor regras sobre os prestadores de tal serviço, a chamada Lei da Restauração da Liberdade na Internet

(*Restoring Internet Freedom Act*) (LEE, 2016). Em 11 de abril de 2016, o presidente da FCC, Tom Wheeler, diz em discurso, em um evento da associação comercial de redes, a INCOMPAS, que a política de taxa zero está sendo revista e que não há uma data final definida (FCC, 2016c). E, ainda, em 15 de abril de 2016, a Câmara dos Deputados dos Estados Unidos aprovou, com apoio bipartidário, a Lei HR 2.666, proposta pelo congressista Adam Kinzinger. Esta Lei refere-se a não regulação de taxa de acesso à Internet de banda larga, e a sua aprovação contém uma forte mensagem para a Casa Branca e para o presidente da FCC, Tom Wheeler, que as taxas de banda larga devem ser mantidas livres de regulação governamental para os ISPs (KINZINGER, 2016; BRODKIN, 2016b; KINZINGER, 2016a).

Em 14 de junho de 2016, a Corte de Apelação do Distrito de Columbia, afirmou que a FCC exerceu sua apropriada autoridade quando reclassificou o acesso à Internet de banda larga como um serviço de telecomunicações sob o Título II da Lei das Comunicações (KARR, 2016).

Em 3 de janeiro de 2017, o projeto de Lei da chamada Lei da Restauração da Liberdade na Internet, do senador Mike Lee, que visava proibir a FCC de reclassificar o serviço de acesso à Internet como um serviço de telecomunicações e de impor regulamentos sobre os prestadores desse serviço, teve seu prazo expirado e não foi promulgado (S. 2602 (114th)..., 2017). Também em 3 de janeiro de 2017, a Lei HR 2.666, que visava a não regulação de taxa de acesso à Internet, também teve seu prazo expirado e não foi promulgada (H.R. 2666 (114th)..., 2017).

Em 3 de fevereiro de 2017, o comissário Michael O'Rielly (FCC, 2017d) declara que a FCC conclui os inquéritos efetuados sobre a taxa zero sem penalizar os ISPs que faziam parte do inquérito. Também em 3 de fevereiro de 2017, o atual presidente da FCC Ajit Pai (FCC, 2017a), declara sobre a prática da taxa zero, que ela aumentou a concorrência no mercado sem fio. Disse também, que a FCC não irá se concentrar em negar esta prática aos consumidores, em vez disso, irá se concentrar em expandir a implantação de banda larga e incentivar ofertas de serviços inovadores.

E, ainda, em 3 de fevereiro de 2017, Ajit Pai (FCC, 2017b) faz uma declaração crítica sobre as regras adotadas para a Internet Aberta em 26 de fevereiro de 2015, aprovadas pela presidência da FCC anterior a ele. Regras que chamou de "regulamentos da meia-noite" que, segundo ele, deveriam ser revogadas.

Em 27 de abril de 2017, a FCC lança uma consulta pública para a sua nova proposta de regulamentação (*Notice of Proposed Rulemaking* (NPRM)). Esta proposta,

que visa a alteração das normas aprovadas pela FCC em 2015, é justificada com a alegação que arriscam a inovação, servindo, em última instância, para ameaçar a Internet aberta que pretendiam preservar. Dentre as mudanças propostas estão: (i) restabelecer a classificação de serviço de informação para o serviço de acesso à Internet de banda larga e regressar ao quadro regulamentar estabelecido numa base bipartidária durante a administração do ex-presidente Bill Clinton; (ii) retornar autoridade à Comissão Federal de Comércio (*Federal Trade Commission*) para policiar as práticas dos ISPs (FCC, 2017c).

Diante disso, organizações como a *Save the Internet* (SAVE THE INTERNET, 2017) e a *Public Knowledge* (PUBLIC KNOWLEDGE, 2017), disponibilizaram petições para serem assinadas por usuários finais em seus *sites,* contra esta nova proposta da FCC e em defesa da Neutralidade da Rede. Em 14 de dezembro de 2017, dia anterior à defesa desta tese, os Estados Unidos revoga a sua regulação de 2015. A FCC decide nesta data, por 3 votos à 2, reclassificar o serviço de acesso à Internet de banda larga como um "serviço de informações" e classificar o serviço de acesso à Internet de banda larga móvel como um "private mobile service", que pode ser traduzido como "serviço móvel privado". Além disso, nesta mesma revogação das regras de 2015, a FCC também restaurou a jurisdição da Federal Trade Commission para a fiscalização das práticas dos ISPs (FCC, 2017e; FUNG, 2017).

3.12. ÍNDIA

Em 27 de março de 2015 o órgão regulador do governo da Índia, a TRAI (*Telecom Regulatory Authority of India*) publicou um documento de consulta pública sobre o arcabouço regulamentar dos serviços e aplicações OTT (*Over the Top*). Trata-se de aplicações e serviços acessíveis através da Internet, e de operadores de redes que oferecem serviços de acesso à Internet, como por exemplo, Skype, WhatsApp, Snapchat, Instagram, Google Talk, *sites* de comércio eletrônico (Amazon, Flipkart, entre outros), vídeo *games* e filmes online (Netflix, Pandora). Este documento, de consulta pública, consiste de vinte perguntas e, destas vinte questões, quatro foram especificamente sobre a Neutralidade da Rede, conforme segue: (i) quais são os seus pontos de vista sobre a Neutralidade da Rede, no contexto da Índia? Como devem ser

tratados os seguintes princípios: (a) a concorrência efetiva entre os ISPs; (b) a transparência dos ISPs quanto às suas práticas de gerenciamento de tráfego; (c) os custos de mudança (em um mercado competitivo, o consumidor deve ser capaz de mudar de ISP sem custos indevidos ou outras barreiras); e (d) qualidade de serviço assegurada.

As demais perguntas relacionadas à Neutralidade da Rede são as seguintes. (ii) Quais são as formas de discriminação ou práticas de gerenciamento de tráfego razoáveis e coerentes com uma abordagem pragmática? O que deve ou pode ser permitido? (iii) Deveria ser obrigatório aos ISPs publicarem as várias técnicas de gerenciamento de tráfego utilizadas para diferentes aplicações OTT? Será esta uma condição suficiente para garantir a transparência e um regime regulatório justo? (iv) Como deve ser criado o ambiente propício e equilibrado de tal forma que os ISPs sejam capazes de investir em infraestrutura de rede e os provedores de conteúdo e aplicativos sejam capazes de inovar e crescer? Quem deve arcar com os custos do processo de melhoria da qualidade da rede? (TRAI, 2015a).

Em 16 de abril de 2015, a BBC News relata que o resultado da consulta pública na Índia mostrou que houve apoio à Neutralidade da Rede, com mais de 800.000 indianos enviando e-mails a TRAI, exigindo uma Internet livre e justa (ROY, 2015). Em 9 de dezembro de 2015, a TRAI lança um documento para nova consulta pública sobre a diferenciação de preços dos serviços de dados, convidando as partes interessadas a se pronunciar. Esta consulta pública questionou se os prestadores de serviços deveriam ser autorizados a ter preços diferenciados para o acesso a *sites*, aplicativos ou plataformas e outras questões relacionadas (TRAI, 2015b). Em 27 de dezembro de 2015, o debate sobre a Neutralidade da Rede se mantém intenso em todo o país, após o ISP indiano Airtel, ter decidido cobrar separadamente pelas ligações telefônicas baseadas na Internet. Houve protestos, e os ativistas e especialistas da Internet conseguiram impedir que fosse implantado na Índia este serviço, chamado de Airtel Zero, juntamente com o projeto Internet.org, do Facebook (NET..., 2015b). Em 07 de janeiro de 2016, encerrou o prazo para as manifestações da consulta pública (TELL TRAI..., 2015). E, em 8 de fevereiro de 2016, a TRAI, após ter recebido e divulgado em seu *site* as opiniões recebidas sobre as questões colocadas na consulta pública, emite um regulamento proibindo as práticas de taxa zero, ou as tarifas discriminatórias para os serviços de dados. Desta forma, a TRAI proíbe na Índia a cobrança de diferentes tarifas por prestadores de serviços, para os serviços de dados

baseados nos conteúdo acessados, transmitidos ou recebidos pelo consumidor, e impõe penalidades aos ISPs, em caso de descumprimento do regulamento (TRAI, 2016).

3.13. UNIÃO EUROPEIA

Em 30 de junho de 2015, o Parlamento Europeu, o Conselho Europeu, e a Comissão Europeia, chegam a um acordo sobre as regras necessárias para garantir uma Internet aberta (EUROPEAN COMMISSION, 2015). Antes disso, entre 2009 e 2014, a União Europeia vinha normatizando a Neutralidade da Rede por meio de seus representantes: a Comissão Europeia, o Parlamento Europeu, o Conselho Europeu, e o BEREC. Estas normatizações envolveram questões como o lançamento pela Comissão Europeia, em 20 de novembro de 2009, das ditas 12 reformas das telecomunicações da União Europeia visando assegurar direitos mais fortes para o consumidor, uma Internet aberta, um único mercado europeu das telecomunicações, e conexões de Internet de alta velocidade para todos os cidadãos (EUROPEAN COMMISSION, 2009). Em 25 de novembro de 2009, o Parlamento cria poderes de salvaguarda para as autoridades reguladoras nacionais a fim de evitar a degradação dos serviços e a obstrução ou o retardamento do tráfego nas redes públicas (EUROPEAN PARLIAMENT, 2009). Destaca-se que, também em 25 de novembro de 2009, o Parlamento Europeu e o Conselho Europeu criaram o BEREC, Organismo de Reguladores Europeus das Comunicações Eletrônicas (REGULATION..., 2009). Em 30 de junho de 2010, a Comissão Europeia lança consulta pública sobre as questões fundamentais da Neutralidade da Rede (EUROPEAN COMMISSION, 2010). Em 11 de novembro de 2010, a Comissão e o Parlamento Europeu organizam uma reunião de cúpula para dar oportunidade às partes interessadas no debate da Neutralidade da Rede, de mostrar os seus pontos de vista em um fórum aberto e público (KROES, 2010).

Em 19 de abril de 2011, a Comissão Europeia, a partir do resultado da consulta pública e da reunião de cúpula, elenca os principais pontos discutidos para a Internet aberta e a Neutralidade da Rede na Europa, e os envia ao Parlamento e demais órgãos representativos, a fim de verificar eventual necessidade de orientações suplementares (EUROPEAN COMMISSION, 2011). Em 17 de novembro de 2011, o Parlamento Europeu observa que nesta fase não há necessidade de intervenção regulamentar adicional em nível europeu sobre a Neutralidade da Rede, e solicita transparência no

gerenciamento do tráfego efetuada pelos ISPs, incluindo uma melhor informação para os usuários finais (EUROPEAN PARLIAMENT, 2011). Em 3 de dezembro de 2012, o BEREC publica as orientações sobre a avaliação da razoabilidade das práticas de gerenciamento de tráfego efetuada pelos ISPs, e as restrições relacionadas (BEREC, 2012b). Em 5 de setembro de 2013, a *Open Forum Europe*, uma organização sem fins lucrativos, realiza uma pesquisa junto aos Estados-membros para obter uma posição oficial de cada um sobre a regulamentação da Neutralidade da Rede, independentemente se a favor ou contra ela (OLMOS; CASTRO, 2013). E, em 14 de julho de 2014, a Comissão Europeia apresenta a situação da Neutralidade da Rede na Europa, país a país, a respeito do estado de implementação do seu quadro regulatório (EUROPEAN COMMISSION, 2014).

Finalmente, em 30 de junho de 2015, a Comissão, o Parlamento e o Conselho Europeus, chegam a um acordo sobre os elementos-chave para um mercado único de telecomunicações para os 28 Estados-membros. Dentre as regras propostas destacam-se pela sua inerência à Neutralidade da Rede as seguintes. (i) Não haverá nenhum bloqueio ou estrangulamento de conteúdo *online*, aplicações e serviços. (ii) Cada europeu poderá ter acesso à Internet aberta e todos os provedores de conteúdo e de serviços devem ser capazes de fornecer os seus serviços através de uma Internet aberta de alta qualidade. (iii) Todo o tráfego será tratado de forma igual. Isto significa, por exemplo, que não poderá haver priorização paga de tráfego no serviço de acesso à Internet. Ao mesmo tempo, a igualdade de tratamento permite o gerenciamento de tráfego razoável no dia-a-dia, de acordo com requisitos técnicos justificados, e que deve ser independente da origem ou do destino do tráfego. (iv) Será permitida a prestação de serviços especializados ou inovadores, desde que eles não prejudiquem o acesso à Internet aberta. Tais serviços incluem o IPTV, a videoconferência, ou os serviços de saúde de alta definição, como a telecirurgia. (v) Taxa zero: também chamada na União Europeia de conectividade patrocinada, a taxa zero é considerada pela Comissão, Parlamento e Conselho Europeus como uma prática comercial utilizada por alguns provedores de acesso à Internet, nomeadamente os operadores móveis, para não contar o volume de dados de aplicativos particulares na quota mensal limitada do usuário (EUROPEAN COMMISSION, 2015).

Em 26 de outubro de 2015, Tim Berners-Lee ressalta que esta proposta é fraca e confusa porque permite aos ISPs: (i) criar “pistas rápidas”, cobrando das empresas para fornecerem conteúdos priorizados na forma de serviços especializados; (ii) isentar

algumas aplicações da quota de dados dos usuários da Internet, novamente chamada de taxa zero; (iii) definir classes de serviços, acelerando ou desacelerando o tráfego destas classes; e (iv) retardar o tráfego a qualquer hora, argumentando, por exemplo, que o congestionamento estava prestes a acontecer, portanto, estava impedindo este iminente congestionamento. Para Tim Berners-Lee, se essas regras propostas forem adotadas como estão, irão ameaçar a inovação, a liberdade de expressão e a privacidade, e comprometer a capacidade de liderança da Europa na economia digital. Mais de trinta empresas como BitTorrent, Netflix e reddit e organizações como Bits of Freedom e Electronic Frontier Foundation, assinaram uma carta aberta ao Parlamento Europeu para aprovar as alterações necessárias para impedir que os ISPs possam ter este comportamento nocivo à Neutralidade da Rede (WORLD WIDE WEB FOUNDATION, 2015). Em 27 de outubro de 2015, o Parlamento Europeu levou à votação as alterações propostas e votou contra elas, deixando a responsabilidade para as autoridades reguladoras dos Estados-membros. O BEREC é quem deverá emitir as diretrizes, após consulta pública (BARANIUK, 2015) e (THE FIGHT..., 2015).

Em 30 de agosto de 2016 o BEREC (BEREC, 2016b) lança as diretrizes da Neutralidade da Rede para as autoridades reguladoras nacionais (*National Regulatory Authorities* (NRAs)), dos países que fazem parte da União Europeia. Estas diretrizes fornecem as orientações necessárias para as autoridades, as NRAs, terem em conta quando da aplicação das regras e da avaliação de casos específicos. Para chegar a estas diretrizes o BEREC lançou uma consulta pública de seis semanas, que encerrou em 18 de Julho de 2016. O número de contribuições recebidas antes da data-limite foi de 481.547, resultando em uma participação sem precedentes para uma consulta do BEREC. As contribuições foram provenientes de diversas categorias: da sociedade civil, instituições públicas e peritos independentes, ISPs, fornecedores de conteúdos e aplicações, e outras partes interessadas da indústria. O BEREC processou as contribuições recebidas e realizou uma avaliação exaustiva das contribuições, atualizando cerca de um quarto dos parágrafos das diretrizes para a sua versão final.

De acordo com a *Save the Internet* (EU..., 2016), as orientações finais do BEREC, que foram publicadas em 30 de Agosto de 2016, oferecem algumas das proteções de neutralidade de rede mais fortes que se poderia desejar. Sendo estas novas regras devidamente aplicadas pelos reguladores nacionais de telecomunicações, elas representam uma vitória retumbante para a Neutralidade da Rede. O *site* esclarece que a sociedade civil deve ficar atenta e observar que os operadores de telecomunicações não

violem os novos princípios. O *site* finaliza ressaltando que o resultado desta regulação do BEREC deveu-se ao esforço excepcional de participação que ocorreu na consulta pública para proteger a Internet livre e aberta.

Com esta nova regulação a ser seguida pelas NRAs, o BEREC visa assegurar o cumprimento das regras destinadas a salvaguardar o tratamento igual e não discriminatório do tráfego na prestação de serviços de acesso à Internet e os direitos dos usuários finais. Dentre as questões tratadas pelo BEREC, destacam-se três, pela sua relevância ao debate da Neutralidade da Rede: (i) taxa zero; (ii) gerenciamento de tráfego; e (iii) transparência (BEREC, 2016a).

(i) Taxa zero. Conforme mencionado anteriormente, é por meio da prática comercial chamada taxa zero que um ISP aplica um preço de zero ao tráfego de dados associado a uma determinada aplicação ou categoria de aplicações (e os dados não contam para qualquer limite de dados no serviço de acesso à Internet). Existem diferentes tipos de práticas de classificação zero que podem ter efeitos diferentes nos usuários finais e na Internet aberta e, por conseguinte, nos direitos dos usuários finais protegidos pelo regulamento do BEREC.

O ISP pode aplicar ou oferecer classificação zero a uma categoria inteira de aplicações (por exemplo, todas as aplicações de vídeo ou de música) ou apenas a determinadas aplicações (por exemplo, os seus próprios serviços, uma aplicação de meios de comunicação social específica, o vídeo mais popular ou aplicações de música). Neste último caso, o usuário final não é impedido de utilizar outras aplicações de música. No entanto, o preço zero aplicado ao tráfego de dados da aplicação de música com pontuação zero (e o fato de o tráfego de dados da aplicação de música com pontuação zero não contar para qualquer limite de dados no serviço de acesso à Internet) cria um incentivo econômico para o uso desse aplicativo de música em vez de outros concorrentes. Os efeitos dessa prática adotada para uma aplicação específica podem minar a essência dos direitos dos usuários finais ou levar a circunstâncias em que a escolha dos usuários finais é reduzida na prática, em comparação à sua adoção para uma categoria inteira de pedidos.

Na avaliação das NRAs sobre tais acordos ou práticas comerciais, como a taxa zero, a avaliação deve ter em conta o objetivo do regulamento de salvaguardar o tratamento igualitário e não discriminatório do tráfego e garantir o funcionamento contínuo do ecossistema da Internet como motor da inovação, bem como a intervenção contra acordos ou práticas comerciais que, devido à sua dimensão, conduzem a

situações em que a escolha dos usuários finais é materialmente reduzida na prática, ou que resulta em minar a essência dos direitos dos usuários finais. A avaliação deve ter em conta também as posições de mercado, dos provedores de serviços de acesso à Internet e dos provedores de conteúdos, aplicações e serviços.

(ii) Gerenciamento de tráfego. Um princípio básico do regulamento do BEREC diz respeito ao gerenciamento de tráfego e a obrigação dos ISPs de tratarem o tráfego de forma equitativa ao fornecerem os serviços de acesso à Internet. As violações deste princípio que não se justificam também constituiriam uma violação dos direitos estabelecidos para o usuário final. Ao avaliar se um ISP cumpre este princípio, as NRAs devem aplicar uma avaliação em duas etapas: na primeira etapa, devem avaliar se todo o tráfego é tratado de forma igualitária e numa segunda fase, devem avaliar se as situações são comparáveis ou diferentes e se existem razões objetivas para justificar um tratamento diferente.

Além disso, as NRAs devem assegurar que o gerenciamento de tráfego nos serviços de acesso à Internet seja sem discriminação, restrição ou interferência; independentemente do remetente e do destinatário, do conteúdo acessado ou distribuído, aplicações ou serviços utilizados ou fornecidos, ou dos equipamentos utilizados.

O objetivo de um gerenciamento de tráfego razoável consiste em contribuir para uma utilização eficiente dos recursos da rede e para uma otimização da qualidade global da transmissão, respondendo a requisitos de qualidade objetivamente diferentes para categorias específicas de tráfego e, portanto, de conteúdos, aplicações e serviços transmitidos. As medidas razoáveis de gerenciamento de tráfego aplicadas pelos ISPs devem ser transparentes, não discriminatórias e não devem basear-se em considerações comerciais. A exigência de que as medidas de gerenciamento de tráfego não sejam discriminatórias não impede que os ISPs implementem medidas que diferenciem categorias de tráfego objetivamente diferentes, a fim de otimizar a qualidade global da transmissão. Tal diferenciação deve ser permitida apenas com base em requisitos de qualidade técnica, objetivamente diferentes (por exemplo, em termos de latência, jitter, perda de pacotes e largura de banda) das categorias específicas, a fim de otimizar a qualidade global e a experiência do usuário do tráfego, e não com base em considerações comerciais. Essas medidas de diferenciação devem ser dimensionadas em relação à finalidade da otimização global da qualidade e devem tratar igualmente o tráfego equivalente. Essas medidas não devem ser mantidas por mais tempo do que o necessário.

São proibidos: bloqueio, desaceleração, alteração, restrição, interferência, degradação e discriminação entre conteúdos específicos, aplicações ou serviços, ou categorias específicas dos mesmos. O BEREC entende que as categorias de tráfego devem ser claramente distinguidas das dos serviços especializados. Esclarece que os serviços especializados podem ser fornecidos por razões de otimização, a fim de satisfazer os requisitos de um nível específico de qualidade.

(iii) Transparência. As NRAs devem procurar assegurar que os ISPs deem transparência às informações sobre o serviço de acesso à Internet que oferecem. Estas informações devem ser claras e compreensíveis: devem ser facilmente acessíveis e identificáveis pelo que são. As informações não devem criar uma percepção incorreta do serviço prestado ao usuário final e devem permitir comparações com o serviço prestado por diferentes ISPs. As NRAs devem assegurar que os ISPs incluam no contrato e publiquem as informações em duas partes, de acordo com o nível de detalhe. A primeira parte deve fornecer informações de nível geral. Isto inclui, por exemplo, uma explicação sobre as velocidades, exemplos de aplicações populares que podem ser usadas com qualidade suficiente, e uma explicação de como tais aplicações são influenciadas pelas limitações do serviço de acesso à Internet. E a segunda parte consiste nos parâmetros técnicos mais detalhados e seus valores, e outras informações relevantes exigidas nestas Diretrizes.

3.14. AUSTRÁLIA

Na página do órgão regulador das telecomunicações da Austrália, a ACMA (*Australian Communications and Media Authority)*, foram encontrados documentos de discussão sobre a regulação referente a alguns serviços como VOIP (ACMA, 2009); OTT (ACMA, 2014); e Internet das Coisas (*Internet of Things*) que se refere à interconexão de muitos dispositivos e objetos utilizando protocolos da Internet (ACMA, 2015). Embora estes documentos citem e tragam considerações sobre a Neutralidade da Rede, nenhum tipo de normatização pertinente ao tema foi encontrada. Em 18 de novembro de 2015, Ziggy Switkowski , presidente da NBN, a Rede Nacional de Banda Larga da Austrália, *National Broadband Network*, diz que é inevitável um debate nacional sobre a Neutralidade da Rede na Austrália, como resultado da largura de banda crescente usada pelos serviços OTT de vídeo, como a Netflix (SADAUSKAS, 2015).

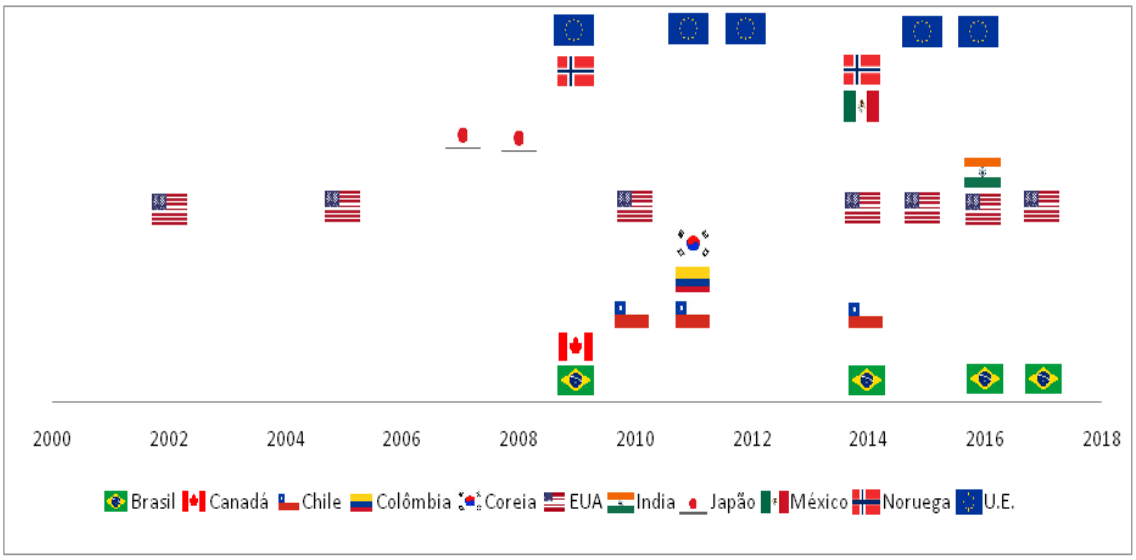
3.15. ÁFRICA DO SUL E QUÊNIA

Tanto na página do atual órgão regulador das telecomunicações da África do Sul, a ICASA (*Independent Communications Authority of South Africa*) (ICASA, 2017), quanto na página do órgão regulador das telecomunicações do Quênia, *Communications Authority of Kenya* (COMMUNICATIONS AUTHORITY OF KENYA, 2016), não foi encontrado qualquer tipo de normatização ou qualquer menção referente ao tema da Neutralidade da Rede. Em 24 de fevereiro de 2016, o ministro queniano da informação, comunicações e tecnologia, Joe Mucheru, afirma que a universalizar o acesso à Internet pelos africanos é mais importante do que defender a Neutralidade da Rede, que "é um problema do mundo desenvolvido" (HILL; MARTINEZ, 2016).

3.16. CONSIDERAÇÕES FINAIS

A Figura 2, abaixo, visa mostrar um contexto temporal onde os pontos marcados com as bandeiras dos países correspondentes, representam os anos nos quais ocorreu algum tipo de estabelecimento de normatização propriamente dita para a Neutralidade da Rede. Nesta figura é possível observar que os Estados Unidos dão o início à regulamentação e também permeiam todo o tempo em que perdura o debate e a regulação no mundo. É possível observar também que há um forte crescimento do número de regulações a partir de 2009. E, é possível observar ainda, que a concentração de um maior número de países efetuando a sua regulação para a Neutralidade da Rede ocorreu em 2011, 2014 e 2016.

FIGURA 2 - LINHA DO TEMPO DA NORMATIZAÇÃO DA NEUTRALIDADE DA REDE NO MUNDO



Fonte: O autor (2017).

À luz do que foi apresentado, verifica-se que o panorama regulatório acerca da Neutralidade da Rede demonstra a preocupação da maioria dos países com a permanência de uma Internet aberta e de livre trânsito, e com a manutenção da concorrência e da inovação. E, em termos específicos, é possível inferir que a preocupação desses países se volta para os aspectos técnicos da gestão da rede para impedir o bloqueio, o estrangulamento, a diferenciação e a priorização. Ao mesmo tempo, é possível inferir também, que a preocupação desses países que estabeleceram regras em defesa da Neutralidade da Rede, é de impedir a prática da taxa zero que, sob o ponto de vista técnico, também se constitui em diferenciação e priorização. E, ainda, há o gerenciamento do tráfego, cuja prática, se for efetuada de forma razoável pelos ISPs, é o que, em termos técnicos, pode garantir a aplicação da Neutralidade da Rede de forma efetiva.

Outro ponto relevante a ser observado é a manutenção do estado de ebulição do debate em torno da Neutralidade da Rede. Mesmo levando em conta toda a preocupação mundial sobre o tema, traduzida pelos governos em regras, Leis ou diretrizes para manter a rede neutra, restam enormes lacunas. O jogo de interesses que norteia o comportamento dos agentes envolvidos no debate é o que impera. Exemplos disso são os Estados Unidos e o Brasil. Mesmo após o estabelecimento de regras rígidas em prol da Neutralidade da Rede, mudanças de governo provocam novamente a inserção de questionamentos à mudança no que foi estabelecido, ou de nova consulta pública, numa

clara demonstração do jogo de interesses existente no mercado das telecomunicações, a quem as regras foram impostas.

CAPÍTULO IV

FERRAMENTAS COMPUTACIONAIS DE DETECÇÃO DE VIOLAÇÃO À NEUTRALIDADE DA REDE

O objetivo deste capítulo é apresentar ferramentas computacionais que podem detectar algum tipo de violação da Neutralidade da Rede, de acordo com os preceitos estabelecidos na normatização desta matéria, e expostos no Capítulo 3. O critério adotado para selecionar e listar estas ferramentas é o da funcionalidade. Dito de outro modo, este capítulo tem por objetivo mostrar as ferramentas computacionais que permitem detectar algum tipo de manipulação indevida no gerenciamento do tráfego, efetuada pelos ISPs, que representam algum tipo de violação ao que foi estabelecido em termos mundiais, na normatização da Neutralidade da Rede. Para efeitos deste capítulo, entende-se por ferramenta computacional, qualquer mecanismo computacional utilizado para o monitoramento do tráfego, ou seus sinônimos, tais como software, técnicas, soluções, códigos, instrumentos, infraestruturas, modelos, aplicativos ou algoritmos.

As ferramentas computacionais estão organizadas da seguinte forma: na Seção 4.1 são apresentadas as ferramentas para detecção de diferenciação de tráfego e na Seção 4.2 são apresentadas outras ferramentas que podem ser usadas no contexto da Neutralidade da Rede. Na Seção 4.3 são apresentadas as considerações finais.

4.1. FERRAMENTAS PARA DETECÇÃO DE DIFERENCIAÇÃO DE TRÁFEGO

O objetivo desta seção é destacar todas as ferramentas computacionais encontradas, projetadas para detectar algum tipo de diferenciação no tráfego da Internet, que represente violação à Neutralidade da Rede. A diferenciação de tráfego é uma das práticas utilizadas pelos ISPs e vedada na normatização da Neutralidade da Rede. As práticas de diferenciação de tráfego podem resultar em uma maior perda de pacotes ou menor largura de banda para a aplicação discriminada, entre outros possíveis fenômenos. As ferramentas existentes para detecção de diferenciação de tráfego, em

geral, baseiam-se em medições de rede diversas, tais como perda de pacotes, largura de banda ou atraso, para inferir se um determinado tipo de tráfego está sendo discriminado em relação a outros. Este tipo de violação da Neutralidade da Rede tem impacto direto sobre o usuário final da rede. Além disso, a competitividade e a inovação na Internet também podem ser prejudicadas por práticas de diferenciação. Porém, detectar se um tipo de tráfego é tratado com menor prioridade em relação a outros não é uma tarefa trivial. Diversos fatores além das práticas de diferenciação podem resultar em uma diferença no desempenho medido para tipos de tráfegos diferentes. Exemplos incluem: características das rotas utilizadas, tráfego de fundo, mudanças constantes nas condições da rede, além das próprias limitações das técnicas de medição utilizadas. Assim, esta seção é focada em ferramentas existentes para detecção deste tipo de violação, e é subdividida da seguinte forma. Na Subseção 4.1.1 são apresentadas as ferramentas Glasnost, BTTest e BonaFide. Na Subseção 4.1.2 são apresentadas as ferramentas NetPolice e NVLens. Na Subseção 4.1.3 é apresentada a ferramenta DiffProbe. Na Subseção 4.1.4 é apresentada uma estratégia baseada em inferência da Neutralidade da Rede. Na Subseção 4.1.5 é apresentada a ferramenta NANO. Na Subseção 4.1.6 é apresentada a ferramenta Gnutella RSP. Na Subseção 4.1.7 é apresentada a ferramenta Packsen. Na Subseção 4.1.8 é apresentada a ferramenta ChkDiff. Na Subseção 4.1.9 é apresentada a ferramenta POPI. Na Subseção 4.1.10 é apresentada uma solução para detecção de diferenciação de tráfego baseada em VPN.

4.1.1. Glasnost, BTTest e BonaFide

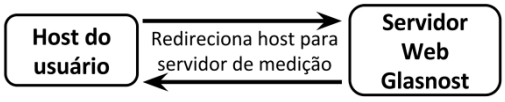
Glasnost (DISCHINGER et al., 2010) é uma ferramenta que permite a usuários finais da Internet detectarem se seus ISPs estão praticando diferenciação do tráfego de dados de diferentes aplicações. O sistema já foi utilizado por milhares de usuários ao redor do mundo, incluindo usuários residenciais sem conhecimento técnico. A ferramenta foi inicialmente aplicada para detecção de diferenciação de tráfego BitTorrent, mas pode também ser utilizada para qualquer outro protocolo de aplicação.

A ferramenta Glasnost foi projetada para ser de fácil utilização por qualquer usuário, independentemente de seu conhecimento técnico. O funcionamento da Glasnost é ilustrado na Figura 3. Primeiramente o usuário acessa a página Web da ferramenta e é redirecionado para um servidor de medição, como mostra a primeira parte da Figura 3.

Existem vários servidores de medição e os usuários são redirecionados dinamicamente para um destes servidores, tornando difícil para os ISPs empregarem medidas contra servidores específicos. O navegador do usuário obtém então a aplicação cliente do Glasnost, como ilustrado na segunda parte da Figura 3. A aplicação cliente é um *applet* Java executado pelo navegador do usuário que conecta-se ao servidor de medição e emula uma sequência de fluxos de dados, efetuando os testes de taxa de transferência para diferentes aplicações, como mostra a terceira parte da Figura 3. Cada teste é composto por dois fluxos de dados em sequência. Um destes fluxos corresponde à aplicação sendo testada, sendo constituído pelo protocolo e dados específicos da aplicação. O outro fluxo é idêntico ao primeiro em quantidade de mensagens, ordem e tamanho dos pacotes, porém com conteúdo definido de forma aleatória, servindo como um *baseline* para comparação com o fluxo da aplicação. A partir da medição da taxa de transferência dos diferentes fluxos, é possível detectar se um ISP está praticando diferenciação de tráfego baseada no conteúdo das mensagens, como descrito abaixo.

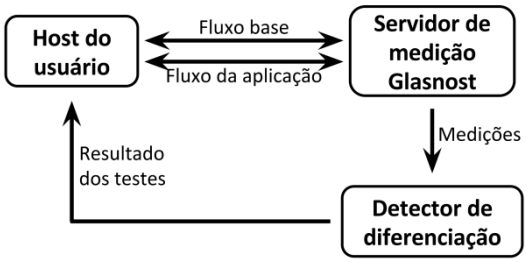
FIGURA 3 - FUNCIONAMENTO DA FERRAMENTA GLASNOST

[Usuário redirecionado para um servidor de medição.]



[Obtenção da aplicação cliente.]

[Execução de testes de taxa de transferência.]



Fonte: O autor (2017).

Cada fluxo de dados entre a aplicação cliente e o servidor de medição dura diversos segundos, tempo suficiente para que o TCP chegue a uma taxa de transferência

estável. Os testes são repetidos múltiplas vezes, a fim de diminuir o ruídos nas medições obtidas. Ao término da série de testes, o servidor de medição processa os dados obtidos e mostra uma página de resultados ao usuário. As métricas computadas são o valor mínimo, máximo e a mediana das taxas de transferência medidas.

Para detectar a diferenciação, a Glasnost verifica se a diferença entre a taxa máxima de transferência dos dois fluxos de dados é maior que um limiar σ. Este limiar é um compromisso entre a capacidade de detectar diferenciação e a produção de falso-positivos (falsas acusações de diferenciação). Se o valor de σ for grande, como 50%, por exemplo, a ferramenta detecta diferenciação apenas se a taxa máxima de transferência de um fluxo for metade da taxa máxima do outro fluxo. Por outro lado, se σ tiver um valor pequeno, 5%, por exemplo, a ferramenta pode erroneamente detectar diferenciação quando houve apenas influência de algum tráfego secundário. Os autores afirmam que 20% é um bom valor para o limiar σ.

Os autores relatam que inicialmente o tempo de cada fluxo de dados era de 60 segundos e cada teste era repetido 5 vezes, fazendo com que o conjunto completo de testes durasse cerca de 20 minutos. Assim, uma grande parcela dos usuários não aguardava o fim dos testes e os interrompiam com menos de 10 minutos de execução. Este problema foi solucionado diminuindo a duração dos fluxos para 20 segundos e repetindo cada teste 2 vezes, resultando em execuções de cerca de 5 minutos.

Os autores relatam que, em 2010, a Glasnost detectou que 10% dos seus usuários sofreram diferenciação no tráfego de BitTorrent. Dentre os casos de diferenciação detectados, a grande maioria ocorreu apenas no envio de dados (*upstream*), com poucos casos de diferenciação detectadas no recebimento (*downstream*) e 20% em ambos. Um resultado surpreendente é que, depois de concluir-se que um ISP estava praticando diferenciação de tráfego, apenas 21% dos usuários do ISP foram efetivamente afetados (mediana). Os autores listam 3 possíveis explicações para este cenário: (i) apenas usuários geradores de uma quantidade grande de tráfego foram afetados; (ii) apenas algumas partes do ISP foram afetadas; e (iii) a diferenciação foi aplicada apenas durante períodos específicos, como horários de pico, por exemplo. Os autores também relatam que cerca de 6% dos usuários alegaram que a ferramenta não detectou diferenciação que eles acreditam estarem sofrendo. Uma possível explicação para isto é que a decisão de minimizar os falso-positivos pode aumentar os falso-negativos.

Outra ferramenta, *trace-emulate*, foi também desenvolvida pelos autores para auxiliar na criação de novos testes para a Glasnost. Esta ferramenta coleta os dados

trafegados de uma aplicação (utilizando uma ferramenta de monitoramento de pacotes) e a partir destes dados cria um teste que pode ser executado na Glasnost para detectar se um ISP está fazendo diferenciação do tráfego da aplicação correspondente.

Uma ferramenta anterior à Glasnost, BTTest (DISCHINGER et al., 2008), foi criada por alguns dos autores da Glasnost e claramente serviu de base para a mesma. O BTTest detecta se um ISP está bloqueando tráfego BitTorrent. O funcionamento do BTTest é muito similar ao do Glasnost, exceto que o BTTest detecta apenas bloqueio de tráfego e apenas para BitTorrent. Para utilizar o BTTest, um usuário acessa uma página Web, na qual um applet Java é executado. Este applet realiza uma série de testes utilizando fluxos de dados diferentes entre o host do usuário e um servidor, assim como é feito pela Glasnost. O BTTest foi disponibilizado por um período de 17 semanas, no qual mais de 47300 usuários finais utilizaram a ferramenta ao redor do mundo. Os dados obtidos neste período foram analisados e concluiu-se que em cerca de 8% dos testes foi detectado o bloqueio de tráfego BitTorrent, principalmente nos EUA. Além disso, a grande maioria dos bloqueios, cerca de 99%, ocorreu no envio de dados (upload) e não no recebimento (download).

Foi também desenvolvida posteriormente por outros autores outra ferramenta similar, BonaFide (BASHKO et al., 2013). BonaFide é uma adaptação da Glasnost focada em detectar diferenciação de tráfego em redes móveis (como 4G, por exemplo). A ferramenta foi desenvolvida para o sistema Android e funciona de forma muito similar a Glasnost: uma aplicação cliente, executada no dispositivo móvel, comunica-se com um servidor de medição executando assim os testes. Cada teste é constituído de 2 fluxos de dados, como no Glasnost. A BonaFide suporta diversos protocolos de aplicação, como VoIP e BitTorrent, por exemplo.

4.1.2. NetPolice e NVLens

A NetPolice (ZHANG; MAO; ZHANG, 2009) é uma ferramenta para detecção de diferenciação de tráfego em um ISP do "núcleo da rede". Os autores afirmam que detectar diferenciação de tráfego no núcleo tem impacto maior do que a detecção nos ISPs que atendem diretamente os usuários finais, já que a diferenciação no núcleo afeta uma quantidade maior de tráfego. A detecção de diferenciação de tráfego da NetPolice

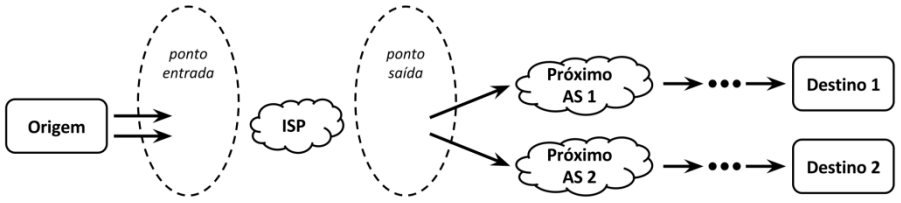
baseia-se na taxa de perda de pacotes, que é medida a partir de diversos pontos de vista – *hosts* finais – em relação a um mesmo núcleo.

A NetPolice detecta diferenciação baseada em conteúdo e em roteamento. A diferenciação baseada em conteúdo ocorre quando os tráfegos gerados por diferentes aplicações são tratados de forma diferente, isto é, de acordo com a porta destino ou conteúdo dos pacotes, um ISP pode dar prioridade maior/menor aos mesmos ou até bloqueá-los. A diferenciação baseada em roteamento ocorre quando pacotes são tratados de forma diferente dependendo dos seus dados de roteamento como, por exemplo, de qual AS veio o pacote ou para qual AS o pacote será roteado.

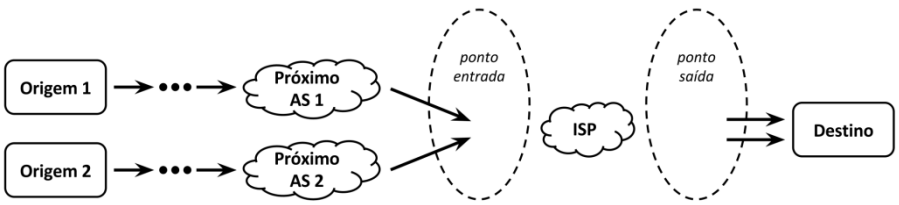
A Figura 4 mostra como a NetPolice detecta cada tipo de diferenciação – baseada em conteúdo e roteamento. Na primeira parte da Figura 4, as medições são feitas usando a mesma origem e destinos diferentes, selecionados de forma que os *hops* imediatamente posteriores ao ponto de saída do ISP correspondam a ASes diferentes. Assim, é possível detectar se o ISP faz diferenciação baseada no próximo AS para o qual o pacote será roteado. Na segunda parte da Figura 4, as medições são feitas usando o mesmo destino e origens diferentes, selecionadas de forma que os *hops* imediatamente anteriores ao ponto de entrada do ISP sejam de ASes diferentes. Desta forma, é possível detectar se o ISP faz diferenciação dependendo do AS anterior à sua rede. Na terceira parte da Figura 4, as medições são feitas usando a mesma origem e destino, mas com pacotes de aplicações diferentes (porta destino e conteúdo). Assim, é possível detectar quando o ISP faz diferenciação baseada no conteúdo dos pacotes.

FIGURA 4 - DETECÇÃO DE DIFERENTES TIPOS DE DIFERENCIAÇÃO NA FERRAMENTA NETPOLICE

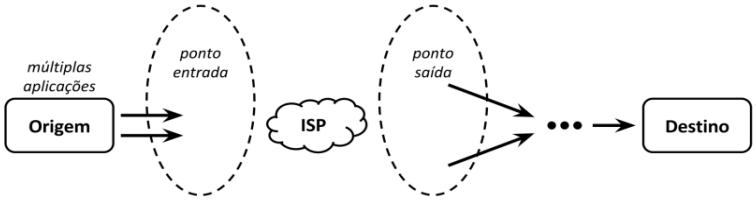
[Detecção de diferenciação baseada no próximo AS.]



[Detecção de diferenciação baseada no AS anterior.]



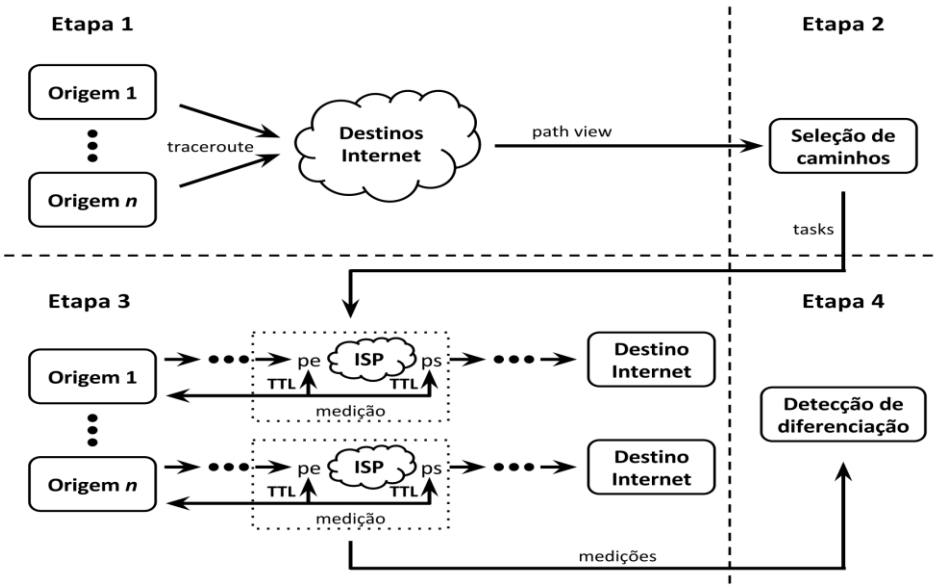
[Detecção de diferenciação baseada em conteúdo.]



Fonte: O Autor (2017).

A detecção de diferenciação do NetPolice baseada nas medições de perda de pacotes segue 4 etapas, ilustradas na Figura 5. A primeira etapa consiste em descobrir todos os caminhos que atravessam o ISP a ser avaliado, a partir de diversas origens (*probers*). Neste processo um grande número de rastreamentos de rota, feitos utilizando o comando *traceroute*, é executado a partir de cada origem e para a maior quantidade possível de destinos na Internet. Assim, além dos caminhos, são também obtidas as distâncias entre os pontos de entrada e saída do ISP, bem como os ASes anteriores e posteriores a estes pontos. Com esta informação, o NetPolice pré-calcula os valores de TTL (*Time to Live*) para alcançar cada par de pontos de entrada e saída do ISP, a partir de todas as origens. O conjunto de caminhos e demais informações obtidas nesta etapa são chamados de *path view*.

FIGURA 5 - FUNCIONAMENTO DA FERRAMENTA NETPOLICE



Fonte: O autor (2017).

Na segunda etapa são selecionados, a partir do *path view* criado na etapa anterior, quais caminhos serão efetivamente medidos, já que não é factível medir todos.

Esta seleção de caminhos a serem medidos deve resultar em uma boa cobertura dos PoPs internos do ISP. A escolha deve ser inteligente, para que não sejam escolhidos origens e destinos que passem pelos mesmos caminhos internos do ISP ou caminhos que não atravessem o ISP. A seleção é modelada como um problema de otimização, com as seguintes restrições: cada tupla *(origem,entrada,saída)* deve ser percorrida pelo menos *R* vezes por caminhos para diferentes destinos; cada tupla *(entrada,saída,destino)* deve ser percorrida pelo menos *R* vezes por caminhos a partir de origens diferentes; e não podem haver mais que *m* caminhos a partir da mesma origem. O conjunto de caminhos a serem medidos é chamado de *tasks*.

Na terceira etapa são feitas as medições dos caminhos selecionados na etapa anterior para diferentes aplicações: HTTP, BitTorrent, SMTP, PPLive e VoIP. A medição de um caminho consiste em, uma vez a cada 200 segundos e para cada aplicação, enviar 2 pacotes: um pacote com o valor de TTL pré-calculado para alcançar apenas o ponto de entrada (pe) e gerar uma resposta ICMP de tempo excedido; e outro pacote com TTL pré-calculado para alcançar o ponto de saída (ps). Assim, subtrai-se a taxa de perda de pacotes do ponto de entrada do ISP da taxa do ponto de saída, obtendo-se a medição apenas para o caminho interno do ISP.

A quarta e última etapa consiste em inferir se cada ISP está fazendo diferenciação de tráfego baseada em roteamento ou conteúdo. Esta inferência utiliza o teste Kolmogorov-Smirnov (KS) para comparar as distribuições dos dados de medição obtidos. A detecção de diferenciação por conteúdo é feita então comparando-se as distribuições de dados de cada aplicação com a distribuição de dados da aplicação HTTP, isto é, testes KS são aplicados para determinar se um conjunto de dados medidos para uma aplicação é significativamente diferente do conjunto de dados para a aplicação HTTP, caracterizando assim uma diferenciação de tráfego. A detecção de diferenciação baseada em roteamento é feita de forma similar, mas comparando-se as distribuições de dados de caminhos diferentes para uma mesma aplicação.

Resultados experimentais com o NetPolice foram obtidos no PlanetLab. Nestes experimentos, 18 ISPs distribuídos em 3 continentes foram estudados em um período de 10 semanas. Os resultados mostraram que 4 ISPs realizaram diferenciação de tráfego em 4 aplicações e 10 ISPs realizaram diferenciação baseada no AS anterior dos pacotes. As taxas de perda de pacotes medidas nestes casos chegaram a ser até 5% diferentes. Os autores também observaram, a partir dos resultados obtidos, que a diferenciação de tráfego pode depender da carga da rede. Já para alguns ISPs, os valores atribuídos ao

campo TOS do cabeçalho dos pacotes tem forte relação com a diferenciação (diferente priorização) e esta atribuição de valores é baseada apenas na porta de destino dos pacotes, não no conteúdo (não é feito DPI). Outra observação foi que a diferenciação de tráfego não é feita de forma homogênea em todos os roteadores dos ISPs.

Um trabalho anterior ao NetPolice foi publicado pelos mesmos autores e apresenta uma versão anterior da ferramenta, com o nome de NVLens (ZHANG; MAO; ZHANG, 2008). No trabalho mais recente (ZHANG; MAO; ZHANG, 2009), os autores detalharam diversos experimentos no PlanetLab, expandiram a análise dos dados obtidos e reformularam a última etapa do processo de detecção (teste para comparação das distribuições de dados).

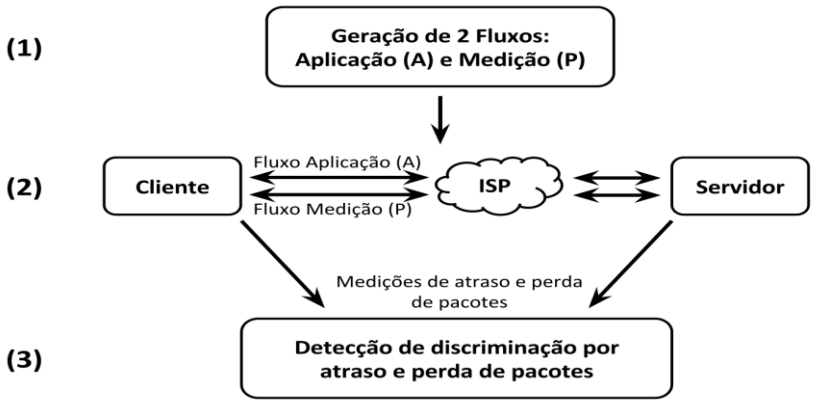
4.1.3. DiffProbe

DiffProbe (KANUPARTHY; DOVROLIS, 2010) é uma ferramenta de detecção de diferenciação de tráfego por atraso e/ou descarte de pacotes. Esta detecção é feita por meio de medições feitas em fluxos de dados simultâneos entre um *host* cliente e um servidor. A ferramenta assume que um ISP classifica cada pacote como sendo de alta prioridade (classe H) ou baixa prioridade (classe L). Os autores afirmam que esta estratégia é genérica e abrange qualquer outro tipo específico de classificação que possa ser empregado por um ISP (baseado em portas, DPI, entre outros). Pacotes classificados como de baixa prioridade (L) podem sofrer atrasos e/ou perdas maiores dependendo das políticas de escalonamento e descarte empregadas pelo ISP.

Idealmente, os roteadores de um ISP devem escalonar os pacotes a serem roteados seguindo a política FCFS (*First Come First Served*) e a política de descarte de pacotes deve ser DT (*Drop-Tail*). Assim, o próximo pacote a ser roteado é sempre o que chegou antes e em caso de *buffer* cheio os próximos pacotes a chegarem são descartados, independentemente da classificação. Assim, todo tipo de tráfego está sujeito às mesmas condições de atraso e perdas. Os autores também afirmam que as políticas de escalonamento e descarte de pacotes só tem um impacto real no tráfego de dados de um usuário quando a rede está congestionada: em momentos em que a rede está com baixa carga, qualquer política de escalonamento irá comportar-se como FCFS e nenhum pacote será descartado, dificultando a detecção de qualquer diferenciação que um ISP possa estar praticando.

O DiffProbe requer 2 agentes: um cliente conectado à rede do ISP a ser verificado e um servidor. O funcionamento da ferramenta pode ser dividido em 3 partes, ilustradas na Figura 6. A primeira parte (1) consiste em um gerador de fluxos de dados. São gerados 2 fluxos diferentes: um fluxo de dados correspondente a uma aplicação suspeita de estar sofrendo diferenciação (A) e outro fluxo de dados de medição (P). Os autores assumem que o fluxo P é do tipo H (alta prioridade) e, portanto, não sofre nenhuma deterioração. A segunda parte é responsável por executar os fluxos de dados. Os fluxos são enviados simultaneamente pela rede, primeiro do cliente para o servidor e em seguida no sentido contrário. A terceira parte (3) da ferramenta é responsável por detectar se houve alguma diferenciação. Nesta detecção são utilizadas as medições de atraso e perda de pacotes, obtidas pelo cliente e servidor. A detecção baseia-se em uma comparação estatística entre as medidas correspondentes a cada fluxo. Estas três partes do DiffProbe são descritas em mais detalhes abaixo.

FIGURA 6 - FUNCIONAMENTO DA FERRAMENTA DIFFPROBE



Fonte: O autor (2017).

O fluxo de dados A é gerado a partir de um fluxo real, pré-armazenado, de uma aplicação. O DiffProbe dá duas opções de aplicação para o usuário: Skype e Vonage. Para criar o fluxo A são mantidos os protocolos de transporte, tamanhos de pacotes, portas, dados e intervalos de envio do fluxo original da aplicação. A geração do fluxo P é baseada no fluxo A, mas com restrições: o fluxo P deve ser suficientemente diferente do fluxo A, garantindo que P não seja classificado da mesma forma que A, ou seja, o fluxo P não pode ser classificado como de baixa prioridade. Por outro lado, o fluxo P deve ter características de rede (como tamanho dos pacotes) similares ao fluxo A para que possam ser posteriormente comparados. Na prática, o DiffProbe cria os pacotes do

fluxo P conforme o fluxo A é enviado. Um pacote qualquer do fluxo P tem o mesmo tamanho do último pacote do fluxo A enviado até então, com dados aleatórios e uma porta com baixa probabilidade de ser considerada de baixa prioridade.

A execução dos fluxos é feita em duas fases. Na primeira fase, os pacotes dos dois fluxos são enviados simultaneamente em uma taxa de envio igual. Na segunda fase, a taxa de envio do fluxo P é aumentada, enviando-se mais pacotes do fluxo P do que do fluxo A. O objetivo desta segunda fase é maximizar a chance de ocorrer enfileiramento de pacotes nos roteadores do ISP, já que, como dito anteriormente, não é possível detectar diferenciação quando a carga da rede é baixa e os roteadores não precisam escalonar os pacotes a serem roteados. O DiffProbe não altera a taxa de envio do fluxo A, pois isso pode alterar a classificação do mesmo (se a classificação for baseada em fluxo, por exemplo). Com o aumento da taxa de envio de pacotes do fluxo P, são coletadas mais medidas para o fluxo P do que para o fluxo A. Assim, para os pacotes do fluxo P, o DiffProbe considera na detecção apenas as medidas referentes aos pacotes enviados imediatamente depois de algum pacote do fluxo A, resultando na mesma quantidade de medidas para os 2 fluxos. A primeira fase serve apenas para verificar se a diferenciação é identificável: os maiores valores de atraso do fluxo P na segunda fase devem ser significativamente maiores que os atrasos médios do fluxo P na primeira fase para que a diferenciação seja estatisticamente identificável.

A detecção de diferenciação por atraso é feita comparado-se as distribuições dos atrasos medidos para cada fluxo: no caso de um escalonamento FCFS, os dois fluxos devem apresentar uma distribuição similar de atrasos dos pacotes. Caso exista despriorização dos pacotes do fluxo A, a distribuição dos atrasos do fluxo A será significativamente maior que a distribuição dos atrasos do fluxo P. O teste de igualdade para as distribuições de atrasos usado pelo DiffProbe baseia-se na divergência de Kullback-Leibler. A detecção de diferenciação por perda de pacotes também é feita comparando-se as distribuições das taxas de perda medidas para cada fluxo, de forma análoga. Porém, o teste de igualdade utilizado pela ferramenta para esta comparação é o teste Z para comparação de duas proporções (*two-proportion z-test*).

Os autores avaliaram o DiffProbe por meio de simulações, utilizando NS2, e da emulação de um ambiente real. Para este ambiente emulado, foram utilizados um cliente conectado a um ISP residencial e um servidor hospedado em uma universidade. A diferenciação foi emulada por um roteador entre o *host* cliente e o ISP. Tanto as simulações quanto os experimentos no ambiente emulado mostraram que, quando a

diferenciação é identificável e o fluxo de medição foi capaz de gerar enfileiramento de mensagens, a detecção foi precisa.

4.1.4. Inferência da Neutralidade da Rede

Em (ZHANG; MARA; ARGYRAKI, 2014) os autores propõem um algoritmo para inferir sobre a Neutralidade de uma Rede qualquer se baseando apenas em observações externas (medições fim-a-fim). O algoritmo também é capaz de identificar especificamente em qual link ou sequência de links a violação da Neutralidade da Rede ocorreu. Os autores fornecem provas formais demonstrando em quais condições o algoritmo atinge estes resultados. O algoritmo foi inspirado em técnicas de tomografia de rede (COATES et al., 2002) que consiste em inferir métricas sobre os links internos de uma rede (como latência e taxa de perda de pacotes, por exemplo) apenas a partir de medições fim-a-fim, ou seja, sem medir diretamente cada link.

A técnica de tomografia de rede utilizada assume que a rede é neutra: cada link trata qualquer tráfego de qualquer rota da mesma forma. Caso isto não ocorra, torna-se impossível expressar as medições de diferentes rotas como função das métricas dos links e o sistema de equações resultante não tem, portanto, solução. Assim, enquanto as técnicas convencionais de tomografia de redes tentam construir sistemas de equações com solução, o algoritmo proposto (ZHANG; MARA; ARGYRAKI, 2014) tenta construir sistemas de equações sem solução, revelando assim violações da Neutralidade da Rede. A ideia central deste algoritmo é que, quando uma rede não é neutra, observações feitas de pontos de vista distintos serão inconsistentes entre si.

A técnica de tomografia utilizada impõe restrições quanto à métrica empregada para realizar as medições entre os *hosts* finais. Esta deve ser aditiva, ou seja, considerando uma rota entre 2 *hosts* finais, a soma dos valores medidos para cada link da rota, utilizando tal métrica, deve ser igual ao valor medido entre os *hosts* finais (a rota toda). Latência e taxa de perda de pacotes são exemplos de métricas aditivas.

O algoritmo recebe como entrada a topologia da rede e um conjunto de medições fim-a-fim com as respectivas rotas entre os *hosts* finais a partir dos quais as medições foram feitas. A saída do algoritmo é um conjunto de sequências de links não neutras, ou seja, quais links, ou sequências de links, violaram a Neutralidade da Rede. As medições entre os *hosts* finais podem ser feitas utilizando em seus pacotes dados de diferentes

aplicações, assim como dados de uma mesma aplicação com origem/destino diferentes. Desta forma, é possível detectar violações da Neutralidade da Rede baseadas tanto no conteúdo quanto na origem ou destino das mensagens.

Como mencionado acima, o algoritmo consiste em buscar sequências de links que geram um sistema de equações sem solução. Para cada sequência de links que esteja presente em mais de uma rota, forma-se um sistema de equações utilizando todas as medições cujas rotas atravessam esta sequência de links. Caso o sistema de equações construído não tenha solução, a sequência de links é não neutra. Caso contrário, a sequência é neutra ou a violação da Neutralidade da Rede para esta sequência de links não é identificável (falso-negativo). Em outras palavras, o algoritmo confronta as medições cujos pacotes atravessaram um mesmo segmento da rede, tentando encontrar inconsistências que podem ser atribuídas a alguma diferenciação ocorrida nestes segmentos.

Os autores afirmam que este algoritmo não gera falso-positivos, ou seja, nunca acusa erroneamente uma sequência de links como não neutra. A razão para isto é que medições que englobam uma sequência de links neutra sempre resultarão em um sistema de equações com solução. Já no caso de falso-negativos, os autores afirmam que ocorrem com pouca frequência. Nestes casos, o algoritmo considera como neutra uma sequência de links que na verdade não é neutra.

Para avaliar o algoritmo, foram feitas duas séries de experimentos em ambientes emulados, com diferentes topologias. Primeiramente foi utilizada uma topologia com um único link discriminatório. Neste experimento, todas as medições foram feitas atravessando este link. Foram testados diferentes cenários, variando o comportamento do link discriminatório. Em todos os casos o algoritmo decidiu corretamente se o link era neutro ou não. Na segunda série de experimentos foi utilizada uma topologia com diversos links discriminatórios. Cada link destes teve um comportamento diferente. Assim como na primeira série, o algoritmo detectou corretamente os links não neutros em todos os experimentos.

Os autores também discutem os desafios para implementar a solução proposta em um ambiente real. A opção mais viável na prática, segundos os autores, é dispor de um conjunto de *hosts* finais que efetuam periodicamente medições das rotas entre eles e enviam estes dados para serem processados em um servidor central. Também é necessário o uso de alguma solução para descobrir a topologia da rede que conecta os

hosts envolvidos nas medições, um requisito do algoritmo. Outro desafio é coletar medições a partir de uma quantidade suficiente de pontos de vista diferentes.

4.1.5. NANO

O NANO (*Network Access Neutrality Observatory*) (TARIQ et al., 2009) é um sistema cujo objetivo é inferir se um ISP está discriminando o tráfego de algum serviço específico. Isto é feito verificando-se se um ISP está causando degradação do desempenho de um serviço quando comparado ao desempenho do mesmo serviço em outros ISPs. Se o desempenho de um serviço medido na rede de um ISP é estatística e significativamente menor que o desempenho do mesmo serviço medido na rede de outros ISPs, é possível que haja uma violação da Neutralidade da Rede. O NANO utiliza um modelo de inferência causal, tentando estabelecer uma relação entre a degradação de desempenho observada e as políticas de um ISP. As medições de desempenho no NANO são obtidas de forma passiva, ou seja, apenas são feitas medições do tráfego real dos serviços observados.

As principais diferenças entre o NANO e outras soluções existentes na época para detecção de violação da Neutralidade da Rede são, segundo os autores: (i) outras soluções detectam discriminação baseada em características específicas como, por exemplo, porta e conteúdo dos pacotes, enquanto o NANO tem um abordagem mais genérica, medindo o desempenho dos serviços independentemente dos mecanismos específicos de diferenciação empregados pelos ISPs; (ii) outras soluções utilizam medições ativas das redes dos ISPs, enquanto o NANO captura suas métricas de forma passiva, o que torna mais difícil para os ISPs detectar e escapar da inferência do NANO; e (iii) as demais soluções comparam métricas de diferentes serviços em um mesmo ISP, enquanto o NANO compara métricas de um mesmo serviço em diferentes ISPs.

A estratégia de detecção de diferenciação do NANO apresenta 3 grandes desafios: (i) o mecanismo de diferenciação empregado pelo ISP pode não ser conhecido, assim a estratégia de detecção precisa ser genérica; (ii) o desempenho padrão de um serviço em um determinado ISP não é conhecido, dificultando a detecção de possíveis degradações, já que não há um valor base para comparação; e (iii) muitos fatores, além da diferenciação de tráfego, podem causar degradação no desempenho de serviços,

como sobrecarga, localização geográfica, software, *hardware* e outras particularidades da rede.

Os diferentes fatores, além da diferenciação de tráfego, que podem causar degradação no desempenho de um serviço, são representados, no modelo estatístico utilizado pelo NANO, por variáveis de confusão (GREENLAND; ROBINS; PEARL, 1999). Assim, é necessário identificar quais são as variáveis de confusão e coletar dados não somente sobre o desempenho de serviços, mas também sobre estas variáveis. A detecção de diferenciação do NANO é feita, portanto, comparando-se o desempenho de um mesmo serviço em ISPs diferentes, usando medições cujas variáveis de confusão são similares. Um exemplo de variável de confusão é o horário do dia: não se deve comparar medições obtidas em horários distintos, já que serviços podem ter um desempenho diferente conforme o horário (devido a uma maior carga, por exemplo).

O NANO utiliza a técnica de estratificação para agrupar as medições de desempenho conforme o valor das respectivas variáveis de confusão. Esta técnica coloca cada medição em um estrato, de forma que as variáveis de confusão referentes a cada amostra em um mesmo estrato têm valores similares. São definidas três categorias de variáveis de confusão: (i) variáveis referentes ao cliente (exemplos incluem softwares que podem afetar o desempenho do serviço medido, como sistema operacional ou um navegador *Web* específico); (ii) variáveis referentes à rede (como localização geográfica, por exemplo); e (iii) variáveis temporais (como o horário do dia, por exemplo, que podem afetar o desempenho do serviço sendo medido).

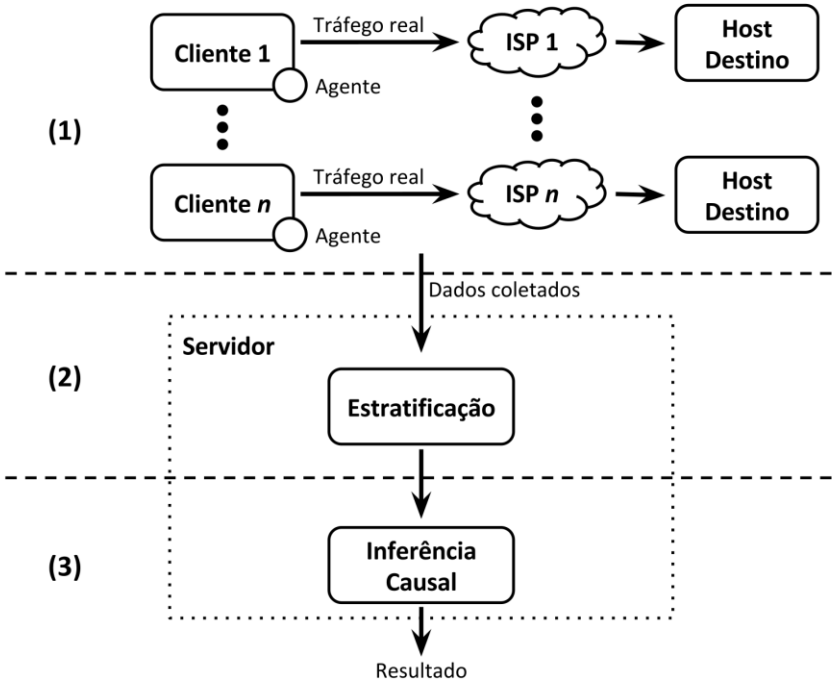
Após a estratificação, o NANO estima, para cada estrato, quanto o desempenho de um serviço muda quando acessado através de um ISP, em relação ao desempenho obtido quando não se utiliza tal ISP – o desempenho médio (*baseline*). O desempenho médio é a média do desempenho de todos os outros ISPs dentro do estrato, excluindo o ISP sendo avaliado. Estas estimativas representam uma quantificação da relação causal entre cada ISP e uma possível diferenciação de tráfego sendo praticada.

A partir das estimativas de cada estrato, o último passo na detecção de diferenciação do NANO consiste em agregar as estimativas de todos os estratos e verificar se os valores obtidos são estatisticamente significativos. A ideia central é que se, na média, o desempenho de um serviço degradou-se significativamente ao utilizar-se um ISP específico, então tem-se uma relação causal entre o ISP e a prática de diferenciação de tráfego.

A implementação do NANO é dividida em duas partes: os agentes e um servidor. Um agente é executado em cada *host* cliente, sendo responsável por monitorar o desempenho do serviço, medindo seu tráfego real a partir do *host* cliente. As métricas utilizadas são específicas de cada serviço, conforme o que for mais adequado para cada um. Além dos dados de desempenho dos serviços, os agentes também coletam os dados referentes às variáveis de confusão. Todos os dados adquiridos pelos agentes são enviados periodicamente para o servidor. Os agentes são implementados como *sniffers* de rede, analisando todos os pacotes recebidos e enviados pelo *host*. Já o servidor do NANO recebe todos os dados coletados pelos agentes e é responsável por realizar a detecção de diferenciação com base nestes dados.

A Figura 7 ilustra o funcionamento do NANO. Em (1) cada cliente executa um agente. Os agentes monitoram o tráfego real dos serviços sendo avaliados. Os dados coletados são enviados para o servidor, que primeiramente os separa em estratos conforme as variáveis de confusão (2). Por fim, o servidor infere (3), seguindo o modelo causal, quais ISPs praticaram diferenciação de tráfego para cada serviço medido.

FIGURA 7 - FUNCIONAMENTO DA FERRAMENTA NANO



Fonte: O autor (2017).

Para avaliar o NANO, os autores conduziram experimentos em um ambiente controlado, utilizando os *testbeds* PlanetLab e Emulab. Foram selecionados nodos do

PlanetLab geograficamente distribuídos. Estes nodos foram utilizados como servidores das aplicações a serem avaliadas. Um conjunto de ISPs foi criado no Emulab, cada um com um conjunto diferente de clientes. Cada ISP fornecia conectividade à Internet para os seus clientes. Assim, todo acesso dos clientes aos serviços hospedados nos nodos do PlanetLab passava por estes ISPs, permitindo a emulação de diferentes práticas de diferenciação e de diferentes variáveis de confusão.

Os resultados dos experimentos mostraram que o NANO é capaz de detectar diferenciação de tráfego praticada de diferentes formas e para diferentes tipos de aplicação, desde que todos os fatores que possam confundir significativamente a relação entre um ISP e o desempenho observado de um serviço – as variáveis de confusão – sejam conhecidos. A estratégia de detecção do NANO mostrou-se genérica o suficiente, detectando a discriminação de tráfego mesmo sem conhecer quais as políticas de diferenciação empregadas pelos ISPs.

Porém, se o NANO não considerar todas as variáveis de confusão, a relação causal entre o ISP e uma possível diferenciação pode ser erroneamente calculada – falso-negativos e falso-positivos. Não há formas automatizadas para enumerar todas as variáveis de confusão pertinentes ou concluir se um conjunto de variáveis de confusão é suficiente, o que pode inviabilizar a aplicação do NANO em um ambiente real.

4.1.6. Gnutella RSP

Os autores (BEVERLY; BAUER; BERGER, 2007) apresentam uma estratégia para quantificar as práticas de bloqueio de portas efetuadas por ISPs na Internet utilizando a rede Gnutella[6]. A estratégia explora o procedimento de ingresso de novos clientes na rede Gnutella para efetuar medições, como descrito abaixo. Foi um dos primeiros trabalhos publicados sobre medições relacionadas à Neutralidade da Rede.

Gnutella é uma rede P2P totalmente descentralizada. Os *hosts* participantes da rede são de 2 tipos: os *superpeers* e as folhas (clientes). Cada *superpeer* é conectado com outros *superpeers* e tem um conjunto de folhas conectadas a ele. Para uma nova folha ingressar na rede, é necessário conectar-se a um *superpeer*. O *superpeer* pode

[6] `http://www.gnutellaforums.com`

aceitar a nova folha, mantendo-a ligada a ele, ou pode informar à folha que está ocupado – caso já tenha muitas folhas, por exemplo. Caso o *superpeer* rejeite a folha, ele indica outro *superpeer* ao qual a folha deve conectar-se para ingressar na rede. Esta indicação contém o endereço IP e a porta TCP do outro *superpeer*.

A estratégia para medição de bloqueio de portas apresentada utiliza 2 *hosts* diferentes: um *host* de medição e um *superpeer* chamado de RSP (*Rogue SuperPeer*). Quando um cliente conecta-se ao RSP para ingressar na rede, o RSP envia uma resposta informando que está ocupado e indica o *host* de medição. O cliente pode então seguir esta indicação e iniciar uma conexão com o *host* de medição na porta indicada. Caso o faça com sucesso, sabe-se então que tal porta não é bloqueada. A ideia central desta estratégia é, portanto, induzir os clientes Gnutella a se conectarem ao *host* de medição para verificar se esta conexão é permitida ou não. Os autores concluiram empiricamente que a probabilidade de um cliente Gnutella não seguir a indicação do RSP, ou seja, não conectar-se ao *host* de medição, é de 80%.

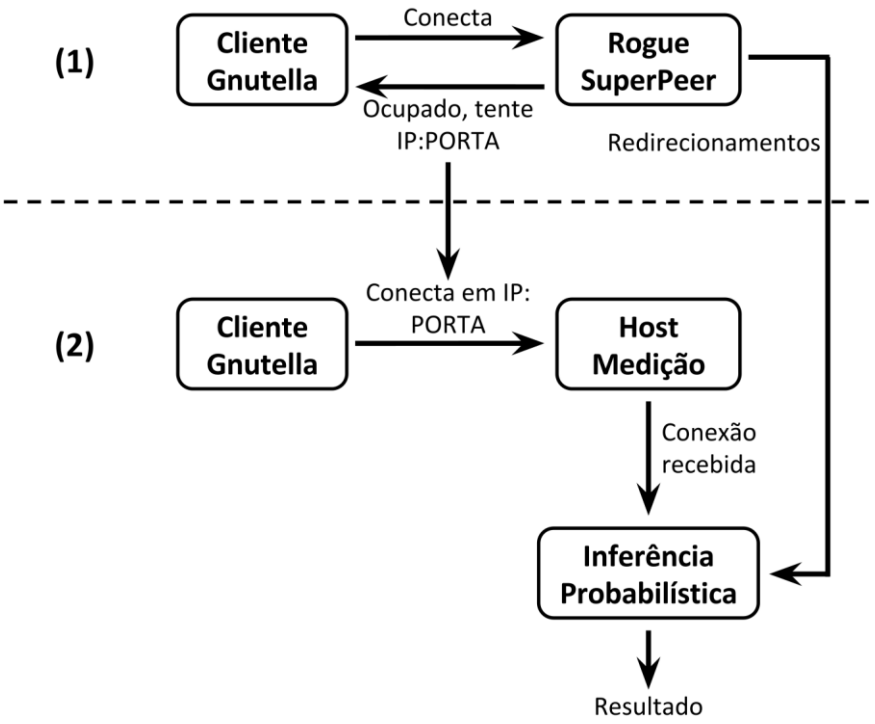
O RSP e o *host* de medição ambos registram as conexões vindas dos clientes Gnutella em um servidor centralizado. Este servidor também é responsável por informar qual porta será indicada aos clientes pelo RSP e qual porta o *host* de medição deverá escutar. O servidor altera esta porta a cada 5 minutos, visando obter dados suficientes sobre todas as portas a serem observadas.

Com base nos dados coletados pelo servidor central é feita uma inferência probabilística para determinar quais portas foram bloqueadas. Note que a estratégia proposta considera que o bloqueio de portas pode acontecer em qualquer ponto entre o cliente e o *host* de medição, não sendo capaz de identificar em que parte do caminho o bloqueio aconteceu. Determinar se uma porta não foi bloqueada é trivial: basta que o *host* de medição tenha recebido pelo menos uma conexão de um cliente Gnutella após a indicação do RSP. Porém, caso nenhuma conexão tenha sido feita com o *host* de medição em uma dada porta, isto não implica que tal porta foi bloqueada. É possível que todos os clientes redirecionados para tal porta não tenham seguido a indicação. Assim, segundo os autores, são necessárias pelo menos 50 indicações para concluir, com probabilidade de 99.5%, que uma porta foi bloqueada.

A Figura 8 ilustra o funcionamento da estratégia. Em (1) um cliente Gnutella conecta-se no RSP a fim de ingressar na rede. O RSP responde o cliente informando que está ocupado, e indica outro *host* (endereço IP e porta) com o qual o cliente deve tentar conectar-se. O *host* indicado pelo RSP é o *host* de medição. O cliente então inicia

uma conexão com o *host* de medição (2). O *host* de medição e o RSP ambos registram as conexões vindas do cliente, informação utilizada para inferir probabilisticamente quais portas foram bloqueadas.

FIGURA 8 - FUNCIONAMENTO DA ESTRATÉGIA RSP



Fonte: O autor (2017).

A estratégia do RSP foi executada durante 2 meses. Neste período, o RSP enviou aproximadamente 150 mil indicações para cerca de 72 mil clientes Gnutella distintos, distribuídos em aproximadamente 31 mil prefixos diferentes – uma fração significativa da Internet. Os resultados mostraram que dos 31 mil prefixos, em 256 houve bloqueio de pelo menos uma porta. A porta bloqueada com maior frequência foi a 136 e as bloqueadas com menor frequência foram a 80 (HTTP), 6346 (Gnutella) e 6969 (observada apenas para comparação). Algumas portas referentes a serviços de email (25, 110 e 143) foram bloqueadas com frequência cerca de duas vezes maior do que a porta 6969. Depois da 136, as outras portas mais frequentemente bloqueadas foram as referentes ao serviços FTP, SSH, Bittorrent e VPNs. Os autores também relatam que algumas universidades e ISPs bloquearam portas de serviços P2P (1214, 4662, 6346, 6881) e alguns ISPs no Canadá, E.U.A. e Polônia bloquearam portas do Skype.

4.1.7. Packsen

Packsen (WEINSBERG; SOULE; MASSOULIE, 2011) é um framework para geração de fluxos de dados utilizado com o objetivo de detectar se um ISP está violando a Neutralidade da Rede por meio da prática de engenharia de tráfego (*traffic shaping*). O Packsen também é capaz de inferir qual o tipo de manipulação de tráfego está sendo empregada e seus parâmetros. A inferência do Packsen é baseada em uma comparação estocástica entre os tempos de chegada dos pacotes de dois fluxos de dados – um fluxo base e um fluxo de medição.

O Packsen considera que um processador de tráfego (*traffic shaper*) mantém múltiplas filas de pacotes, correspondentes a diferentes classes de tráfego. Cada fluxo de dados é classificado em uma das classes, determinando em qual fila os pacotes do fluxo serão inseridos. Esta classificação pode basear-se em diferentes parâmetros, como protocolo de aplicação, porta, hora do dia, origem, destino, entre outros.

Um escalonador determina a forma como os pacotes são retirados das filas de um processador de tráfego e encaminhados. Os escalonadores considerados pelo Packsen são: (i) *First Come First Served* (FCFS), em que não há diferenciação; (ii) *Strict Priority* (SP), em que o escalonador sempre dá prioridade para uma classe específica; (iii) *Leaky Bucket*, em que cada classe tem um limite máximo de largura de banda; (iv) *Token Bucket*, em que cada classe tem um limite para a largura de banda média consumida pelos fluxos; e (v) *Weighted Fair Queuing* (WFQ), em que a largura de banda permitida para cada classe é dividida com base em pesos.

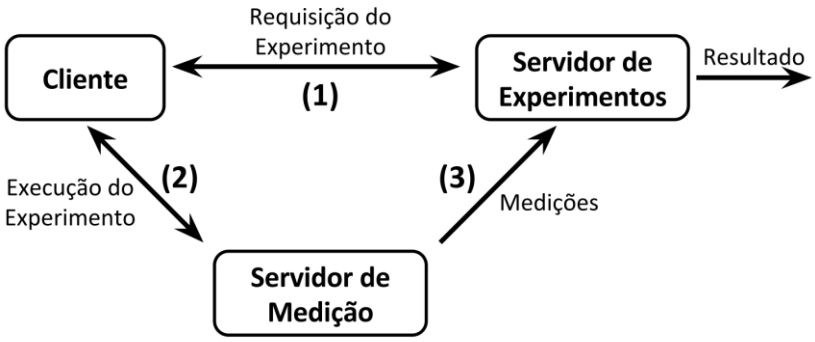
A ideia central da detecção do Packsen é que, quando há discriminação de um fluxo de dados em relação a outro, um dos fluxos apresenta uma alteração significativa quando comparado ao outro. Assim, o Packsen utiliza dois fluxos de dados: um fluxo de medição, referente a aplicações específicas, e um fluxo base, o qual se assume não sofrer nenhuma discriminação. Estes fluxos são enviados entre *hosts* finais de forma intercalada e mantendo a mesma largura de banda para os dois fluxos. Se no recebimento dos fluxos for observada uma diferença significativa entre a largura de banda de cada um, então houve diferenciação de tráfego no caminho entre os dois *hosts*. A métrica utilizada pelo Packsen é, portanto, os tempos de chegada dos pacotes de cada fluxo.

A detecção do Packsen utiliza três métodos. O primeiro método apenas detecta se houve discriminação de um fluxo em relação a outro. Esta detecção é feita

comparando-se as distribuições dos tempos de chegada dos pacotes dos dois fluxos. Se a diferença entre as distribuições for estocasticamente significativa, então houve diferenciação de tráfego. A comparação é feita utilizando o teste U de Mann-Whitney (MANN; WHITNEY, 1947). O segundo método infere qual o tipo de manipulação de tráfego utilizada e quais os parâmetros empregados, como o peso atribuído a cada fluxo, por exemplo. Esta inferência é feita comparando-se a largura de banda dos fluxos no envio com a largura de banda observada no recebimento. Segundo os autores, este método não é robusto na presença de tráfego de fundo (*cross-traffic*). Quando outras aplicações estão gerando uma quantidade significativa de tráfego simultaneamente aos fluxos do Packsen, as larguras de banda dos fluxos podem ser alteradas de forma diferente. É possível que um processador de tráfego classifique o tráfego de fundo e o fluxo de medição como pertencentes à mesma classe, priorizando o fluxo base. Assim, o tráfego de fundo pode influenciar apenas o fluxo de medição e não o fluxo base. O terceiro método trata o tráfego de fundo, sendo capaz de medi-lo, ajustando o monitoramento efetuado. Neste método, as medições do Packsen precisam ser repetidas até que a variação dos resultados seja significativamente baixa.

A implementação do Packsen é dividida em três partes, ilustradas na Figura 9: o cliente, o servidor de experimentos e os servidores de medição. O cliente conecta-se ao servidor de experimentos, solicitando um experimento para ser executado (1). O servidor de experimentos escolhe um experimento em seu repositório e retorna-o ao cliente. O cliente então escolhe um servidor de medição disponível (com baixa carga), informando o experimento que deve ser executado (2). O servidor de medição executa então o experimento, coletando os dados dos fluxos gerados. Os dados são enviados para o servidor de experimentos que os armazena para posterior análise (3).

FIGURA 9 - FUNCIONAMENTO DA FERRAMENTA PACKSEN



Fonte: O autor (2017).

Os autores avaliaram o Packsen primeiramente em um ambiente controlado, utilizando um *testbed* local. Este ambiente permitiu a emulação de diversos tipos de processadores de tráfego, com diferentes parâmetros, assim como diferentes combinações de tráfego de fundo. Após os experimentos no *testbed* local, foram conduzidos experimentos em cerca de 1000 *hosts* do PlanetLab, com o objetivo de melhor avaliar o Packsen em um ambiente real e de maior escala.

Os resultados obtidos no *testbed* local mostraram que o Packsen detectou, com baixa margem de erro, tanto a ocorrência de diferenciação, quanto os parâmetros empregados nos processadores de tráfego, mesmo na presença de tráfego de fundo. Apenas um falso-negativo foi registrado nesses experimentos, no qual houve diferenciação, mas o Packsen não a detectou. Já nos experimentos conduzidos no PlanetLab, foi detectada diferenciação de tráfego em apenas 0.7% dos pares de *hosts* testados (4 de 518).

4.1.8. ChkDiff

ChkDiff (RAVAIOLI; BARAKAT; URVOY-KELLER, 2012; RAVAIOLI; URVOY-KELLER; BARAKAT, 2015) é uma ferramenta para a detecção de diferenciação de tráfego praticada por ISPs que atendem o mercado doméstico. O funcionamento da ferramenta consiste em reproduzir o tráfego real do usuário (previamente capturado e preparado) de forma que este tráfego atinja apenas os

roteadores a poucos *hops* de distância – o ISP do cliente. São efetuadas medições de atraso e perda de pacotes para cada fluxo de dados presente neste tráfego. A partir destas medições, o ChkDiff é capaz de inferir se houve diferenciação e também identificar a partir de qual roteador a diferenciação aconteceu. Os autores afirmam que a estratégia de medição e detecção do ChkDiff é independente de aplicações específicas e das técnicas de engenharia de tráfego utilizadas pelo ISP. Quaisquer que sejam as aplicações discriminadas ou as técnicas utilizadas para tal, uma diferenciação de tráfego tipicamente resultará, para o *host* cliente, em maiores atrasos e perdas de pacotes.

O tráfego de dados utilizado pelo ChkDiff é obtido capturando-se o tráfego real de um usuário durante uma sessão normal de uso (*trace*). Assim, os resultados produzidos pela ferramenta serão referentes ao conjunto de aplicações executadas pelo usuário durante a captura do *trace*. O *trace* capturado é utilizado com o mínimo de alterações: isto garante que os processadores de tráfego (*traffic shapers*) atravessados pelo *trace* terão o mesmo comportamento que teriam caso os pacotes estivessem sendo gerados pelas respectivas aplicações. As únicas modificações feitas nos pacotes de um *trace* são no campo TTL (*Time to Live*), para alcançar apenas o *hop* desejado, e nos dados da aplicação, para que todos os pacotes tenham o mesmo tamanho, evitando assim diferentes tempos de transmissão.

O ChkDiff efetua suas medições reproduzindo o *trace* capturado diversas vezes, a partir do *host* cliente. Utiliza-se um valor incremental para o TTL dos pacotes, de forma que cada reprodução do *trace* alcance o roteador seguinte à reprodução anterior. Quando um pacote chega ao roteador ao qual foi destinado (TTL decrementado para zero), o roteador envia uma mensagem ICMP de tempo excedido (*ICMP Time Exceeded*) de volta ao *host* cliente. As medições de atraso e perda de pacotes utilizadas pelo ChkDiff são referentes a estas respostas ICMP: o atraso é o RTT entre o envio do pacote e o recebimento da resposta ICMP. A perda de pacotes corresponde à taxa de respostas ICMP não recebidas. O objetivo é avaliar apenas os primeiros roteadores após o *host* do cliente, identificando a partir de qual roteador a diferenciação acontece: assume-se a existência de um processador de tráfego logo antes deste roteador.

O ChkDiff faz uma análise estatística para inferir se um fluxo de dados sofreu diferenciação ou não até o roteador destino (para o qual as medições foram obtidas). Compara-se o atraso e perda de pacotes medidos para este fluxo/roteador com os medidos para todo o resto do tráfego até o mesmo roteador. Se estas medições forem significativamente maiores do que as medições do resto do tráfego, então o fluxo sofreu

discriminação a partir daquele roteador. Assim, a base para comparação (*baseline*) utilizada pelo ChkDiff é o tráfego todo: a Neutralidade da Rede estabelece que um fluxo não discriminado é tratado da mesma forma que todo o resto do tráfego, ou seja, as medições obtidas para um fluxo discriminado irão se sobresair em relação ao resto do tráfego. Em um exemplo simplificado, caso a perda de pacotes medida para um fluxo for em torno de 50%, enquanto a perda medida para os demais fluxos for em torno de 10%, é possível que o ISP esteja violando a Neutralidade da Rede.

O ChkDiff foi avaliado primeiramente em um ambiente neutro, sem nenhuma diferenciação, e posteriormente em um ambiente não-neutro. Em ambos, o *trace* do usuário foi capturado durante um período de 3 minutos de uso típico da Internet. Durante este período foram feitos: envios de imagens em uma rede social, navegação em páginas de notícias e envio de mensagens em aplicativos de *chat*.

No ambiente neutro, o ChkDiff foi executado 100 vezes em uma configuração de rede controlada, em que o roteador no segundo *hop* garantidamente não discriminava nenhum dos fluxos presentes no *trace*. Analisando os resultados com apenas 1 reprodução para cada valor de TTL, cerca de 30% das execuções apresentaram de 1 a 3 falso-positivos. Os autores refizeram o experimento, mas com dois *traces* para cada valor de TTL: não houve nenhum falso-positivo. Com base nesta avaliação preliminar, os autores fixaram em 3 a quantidade de *traces* gerados para cada valor de TTL, como descrito anteriormente.

A avaliação em ambiente não neutro foi feita primeiramente com apenas um fluxo discriminado. Posteriormente foram utilizados múltiplos fluxos discriminados, com diferentes frações do *trace* contendo fluxos discriminados. Em ambas as avaliações foi utilizada uma configuração de rede controlada. O *host* do usuário foi conectado a um *host* intermediário (*middlebox*), o qual fornecia acesso à Internet para o *host* cliente e também operava como um processador de tráfego (*traffic shaper*). Este *host* intermediário foi conectado a um roteador, no qual o TTL dos pacotes expirava. Foi utilizada a ferramenta Dummynet (CARBONE; RIZZO, 2010) no *host* intermediário para emular as práticas de engenharia de tráfego. A diferenciação de tráfego foi implementada de duas formas diferentes: limitando a largura de banda dos fluxos selecionados e descartando pacotes dos fluxos selecionados de forma mais frequente.

Nos experimentos com apenas um fluxo discriminado, o ChkDiff foi capaz de detectar corretamente 100% dos fluxos discriminados por limitação de banda. Já quando a diferenciação foi por descarte de pacotes, foram observados alguns falso-negativos

(uma discriminação ocorreu, mas não foi detectada). Nos experimentos com múltiplos fluxos discriminados, a análise estatística do ChkDiff deixou de funcionar corretamente quando a fração de fluxos discriminados é grande (cerca de 80% ou mais). O ChkDiff também foi avaliado na presença de um limite na taxa de envio respostas ICMP do roteador. Os resultados mostraram que o ChkDiff manteve bons resultados na presença de tal limitação.

4.1.9. POPI

A POPI (LU et al., 2010) é uma ferramenta fim-a-fim para inferir se existe priorização no encaminhamento de pacotes de tipos diferentes (*packet forwarding prioritization*). A ideia central do POPI é saturar a banda disponível no caminho entre dois *hosts* finais com pacotes de 2 ou mais tipos diferentes, forçando os roteadores a descartar pacotes quando suas filas estiverem cheias (congestionamento). Em uma rede neutra, todos os pacotes são encaminhados pelos roteadores conforme a ordem de chegada. Assim, caso a rede esteja congestionada e o descarte de pacotes seja necessário, tráfegos de tipos diferentes sofrerão uma taxa de perda similar. Porém, caso os pacotes de um tipo sejam encaminhados pelos roteadores com uma maior prioridade em relação aos pacotes de outros tipos, a taxa de perda de pacotes será diferente, configurando assim uma violação da Neutralidade da Rede.

Os autores afirmam que outras duas métricas também podem ser utilizadas na estratégia do POPI além da taxa de perda de pacotes: o atraso e entrega fora de ordem (*out-of-order*). Estas duas outras métricas geram uma sobrecarga de medição significativamente menor do que a taxa de perda de pacotes. A diferença na taxa de perdas para tráfegos diferentes só pode ser observada quando há congestionamento nos roteadores, fazendo com que pacotes sejam descartados. Assim, é necessário o envio de uma quantidade grande de pacotes para saturar o caminho entre os dois *hosts* da medição, o que não é necessário quando são utilizas as outras duas métricas. Porém, diferenças nas perdas de pacotes podem ser observadas quaisquer que sejam os mecanismos utilizados pelos roteadores para priorizar tipos específicos de tráfego. Atrasos e pacotes fora de ordem não são observados para alguns destes mecanismos. Além disso, diversos outros fatores podem resultar em atrasos maiores e em pacotes

entregues fora de ordem. Um exemplo é o balanceamento de carga, em que os pacotes podem ser roteados para caminhos distintos, resultando em medições de atraso diferentes, não necessariamente relacionadas à alguma discriminação: os pacotes de um caminho podem encontrar roteadores mais lentos do que os pacotes que foram roteados pelo outro caminho, por exemplo. Assim, a justificativa dos autores para utilizar a taxa de perda de pacotes no POPI, apesar da sobrecarga maior na medição, é que esta métrica é capaz de detectar a priorização independentemente do mecanismo de diferenciação utilizado e não é afetada por fatores como caminhos paralelos entre dois *hosts*, sendo assim mais genérica.

Para avaliar o POPI, os autores primeiramente realizaram simulações utilizando o simulador de rede NS2. Nestas simulações foram utilizados dois pares de *hosts* origem/destino. Um destes pares foi responsável por simular o tráfego de fundo, enquanto o outro par simulou a execução do POPI. Na topologia usada nas simulações, a comunicação entre ambos os pares atravessa os mesmos dois roteadores, responsáveis por simular a priorização de determinados tipos de tráfego, com uma largura de banda máxima de 100 Mbps. Os resultados obtidos nestas simulações mostraram que o POPI foi capaz de obter bons resultados mesmo na presença de uma grande quantidade de tráfego de fundo: os pacotes de baixa prioridade foram sempre descartados antes dos de alta prioridade.

Foram conduzidos experimentos no PlanetLab para avaliar o POPI em um ambiente real e encontrar possíveis casos reais de priorização. Nestes experimentos foram utilizados 162 nodos do *testbed*, espalhados em diversos continentes. O POPI foi executado em todos os pares de nodos e em ambos os sentidos para cada par. O tamanho dos pacotes enviados foi de 1500 *bytes* cada, o que gerou um consumo de banda médio de 1.04 Mbps. Os resultados obtidos indicaram que houve algum tipo de priorização de pacotes para 15 pares de nodos. Os autores também executaram o POPI utilizando outras métricas com menor sobrecarga de medição, descritas acima. Os resultados para estas outras métricas mostraram que estas não foram capazes de detectar muitos dos casos de priorização detectados nos experimentos que utilizaram a taxa de perda de pacotes como métrica.

4.1.10 Detecção de Diferenciação de Tráfego Baseada em VPN

Uma solução para detectar diferenciação de tráfego em redes móveis é apresentada em (KAKHKI et al., 2015). O objetivo é medir se uma aplicação arbitrária, executando em dispositivos de usuários finais, como smartphones e tablets, estão sofrendo diferenciação de tráfego. A principal ideia é primeiro capturar o tráfego da aplicação e depois reproduzi-lo duas vezes: uma vez usando uma VPN (túnel criptografado), e uma vez usando um canal convencional não criptografado.

Uma análise estatística é então realizada nas medições obtidas para inferir se havia uma diferenciação de tráfego. As métricas são a taxa de transferência, a perda e o atraso. Neste trabalho, esta solução é chamada de "solução de detecção de diferenciação de tráfego baseada em VPN". Os autores assumem que a diferenciação de tráfego é realizada por um middlebox que executa engenharia de tráfego. A solução de detecção de diferenciação de tráfego baseada em VPN não classifica como diferenciação de tráfego quando a taxa aplicada por estes dispositivos é igual ou superior à taxa na qual o tráfego é gerado. Os autores também assumem que as classificações de tráfego podem ser baseadas em cabeçalho, carga útil ou comportamento do tráfego. Além disso, como a solução emprega uma VPN para reproduzir o traço capturado previamente, também assume que o tráfego VPN é não discriminado.

A solução funciona em três passos. No primeiro passo (1), um servidor VPN captura o tráfego real de uma aplicação móvel enquanto se comunica com o servidor por meio de um túnel criptografado VPN. O traço capturado é então repetido duas vezes no segundo passo (2), desta vez o rastreamento é enviado para um host de medição usando tanto uma VPN (IPSec túnel criptografado), quanto um canal convencional não criptografado. O host de medição obtém informações sobre a taxa de transferência, perda de pacotes e atraso. A detecção de diferenciação é executada na terceira etapa (3), com base nos dados coletados. A solução emprega um teste estatístico baseado em Kolmogorov-Smirnov (KS), a fim de comparar as diferentes distribuições e inferir a presença de diferenciação de tráfego. Segundo os autores, usando uma VPN para capturar o tráfego, eles projetaram uma ferramenta para registrar o tráfego originado de qualquer aplicação móvel sem a necessidade de permissões especiais ou modificações no sistema operacional, já que a ferramenta captura e intermedia a comunicação entre o dispositivo do usuário final e o servidor da aplicação. Contudo, existem algumas limitações potenciais para a solução proposta.

Detectar diferenciação de tráfego somente quando a taxa real é menor do que a taxa de envio do aplicativo pode levar a falsos negativos, especialmente considerando

que a diferenciação de tráfego em geral ocorre quando há congestionamento. Além disso, a solução foi projetada e validada assumindo que a diferenciação de tráfego é implementada por ISPs usando middleboxes que implementam engenharia de tráfego, o que também pode levar a falsos negativos, já que há várias formas de implementar a diferenciação de tráfego. Além disso, o tráfego de fundo pode afetar as medições. A detecção também pode ser dificultada se o próprio tráfego VPN for discriminado pelo ISP. Existem outras soluções para monitorar a Neutralidade da Rede em redes móveis. BonaFide é uma adaptação da Glasnost e aparece descrita anteriormente neste capítulo. WindRider (TRESTIAN; POTHARAJU; KUZMANOVIC, [2017]) é um aplicativo móvel para detectar violações da Neutralidade da Rede em uma rede móvel. Funciona com medições ativas e passivas. As medições ativas são feitas usando a plataforma do MLab (Measurement Lab) (DOVROLIS et al., 2010*).* Várias aplicações usando diferentes portas são geradas entre um dispositivo móvel e um Servidor MLab, a fim de verificar se alguma parte do tráfego está sendo tratada de forma diferente. Medições passivas são tomadas diretamente do dispositivo móvel. A aplicação coleta os atrasos experimentados por diferentes páginas da web, e os comentários explícitos dos usuários finais sobre diferentes aplicações. Os autores (MIORANDI et al.,2013) defendem a criação de um "observatório do cidadão" da Neutralidade da Rede para redes móveis, empregando medições baseadas em *crowdsensing* e no paradigma dos dados abertos. Os autores afirmam que, usando uma abordagem de *crowdsensing* para fazer medições em uma rede móvel, podem aproveitar o crescente número de smartphones, tablets, entre outros dispositivos móveis. Além disso, os autores afirmam que, fazendo todas as medições disponíveis publicamente (abordagem dos dados abertos) permitiu a criação de um "observatório do cidadão", contendo informações relacionadas à Neutralidade da Rede sobre diferentes ISPs, aumentando assim a transparência das redes móveis.

4.2. OUTRAS FERRAMENTAS QUE PODEM SER USADAS NO CONTEXTO DA NEUTRALIDADE DA REDE

Esta seção descreve outras ferramentas relacionadas à Neutralidade da Rede que não se referem diretamente à detecção de diferenciação de tráfego. Estes outros trabalhos tratam de outros tipos de violação da Neutralidade da Rede, como censura ou

qualidade de serviço inferior à contratada, por exemplo, além de outras soluções que podem ser utilizadas no contexto da Neutralidade da Rede.

Ferramentas que medem a qualidade do serviço de ISPs efetivamente entregue ao usuário e/ou monitoram a conformidade do serviço fornecido com acordos de nível de serviço (SLA – Service-Level Agreement), têm relação direta com a Neutralidade da Rede. Existem diversos esforços (BISCHOF; OTTO; BUSTAMANTE, 2012; SÁNCHEZ et al., 2011; AIDA; MIYOSHI; ISHIBASHI, 2003; WHITEBOX, 2015; OOKLA SPEEDTEST, 2015; TESTMY.NET, 2015; SPEEDCHECKER, 2015; SOMMERS et al., 2007; SOMMERS et al., 2010; TA; MAO, 2006; SERRAL-GRACIA et al., 2009; SERRAL-GRACIA et al., 2010; QIU et al., 2008) focados em resolver estas questões, não necessariamente motivados pelo debate da Neutralidade da Rede. Porém, algumas destas ferramentas surgiram devido à preocupação de governos em garantir o cumprimento da Neutralidade da Rede.

A HAKOMetar (WEBER et al., 2013) é uma ferramenta que permite a um usuário final verificar a qualidade de serviço que seu ISP está lhe fornecendo. Esta ferramenta foi desenvolvida pela HAKOM (HAKOM, 2015), a agência reguladora das telecomunicações da Croácia. A estratégia da agência em relação à Neutralidade da Rede é utilizar o HAKOMetar para aumentar a transparência e competitividade no mercado de banda larga do país. O desenvolvimento da ferramenta baseou-se em resultados anteriores acerca de práticas de gerenciamento de tráfego, obtidos em experimentos conduzidos em ambientes de teste na Croácia (JUKIC et al., 2011). A medição do HAKOMetar é feita em três etapas. Na primeira etapa são recolhidos dados sobre o host em que o HAKOMetar está sendo executado e sobre sua rede local. Na segunda etapa, mede-se a taxa de envio e recebimento de dados entre o cliente e o servidor, assim como outras propriedades como latência. Na última etapa, o HAKOMetar cria uma grande quantidade de conexões em paralelo com diversos destinos diferentes, transferindo uma grande quantidade de dados entre o cliente e estes destinos (usando HTTP e/ou FTP). A partir dos resultados da medição, o usuário pode comparar se a largura de banda medida é a mesma que a contratada. Segundo os autores, os resultados reais obtidos com o HAKOMetar indicam que a ferramenta efetivamente aumentou a transparência do mercado de banda larga na Croácia, já que os consumidores passaram a poder verificar se a qualidade do serviço fornecido pelos ISPs estava de acordo com a contratada. Os autores também afirmam que ainda é necessário

incluir mais medições na ferramenta para que ela possa ser usada para detectar violações da Neutralidade da Rede.

A Adkintun (BUSTOS-JIMÉNEZ et al., 2013a) é uma solução para monitoramento da qualidade do serviço de banda larga no Chile. A solução foi desenvolvida pelo *NIC Chile Research Labs* (NIC..., 2015) a pedido da Secretaria Nacional de Telecomunicações do Chile (SUBTEL), com o objetivo de monitorar o cumprimento da Lei da Neutralidade da Rede vigente no país. As medições da Adkintun são efetuadas periodicamente por um software cliente instalado nos hosts dos usuários finais ou embarcado em roteadores residenciais fornecidos a alguns usuários selecionados. Um servidor central informa periodicamente aos softwares cliente quais medições devem ser feitas e quais hosts destino devem ser utilizados nestas medições. As medições da Adkintun incluem disponibilidade, taxa de transferência, latência, perda de pacotes, bloqueio de portas, entre outras. Os hosts destino utilizados nas medições podem estar localizados dentro da infraestrutura do ISP do cliente, em outro ISP chileno ou ainda em uma localização internacional, dependendo da medição. Todas as medições são coletadas por um servidor central, que disponibiliza todos os resultados publicamente em uma página Web. Assim, é possível consultar dados históricos da qualidade de serviço de cada ISP chileno monitorado pela Adkintun. Os autores afirmam que a Adkintun tem proporcionado aos cidadãos meios para proteger seus direitos, já que os resultados obtidos pela ferramenta estão sendo utilizados como base para reclamações de usuários contra a má qualidade dos serviços prestados por ISPs e, até mesmo, como evidência em processos judiciais que envolvem a SUBTEL e ISPs. Também foi desenvolvida uma versão da ferramenta para redes móveis, a Adkintun Mobile (BUSTOS-JIMÉNEZ et al., 2013b; LALANNE et al., 2015). Esta versão utiliza uma combinação de medições passivas com algumas medições ativas efetuadas em dispositivos móveis, com o objetivo de monitorar a qualidade do serviço de Internet móvel no Chile.

Além da qualidade de serviço, a definição de Neutralidade da Rede apresentada anteriormente neste trabalho também trata da liberdade de escolha dos usuários quanto ao conteúdo que desejam acessar. Assim, trabalhos sobre detecção de censura na Internet também têm relação com a Neutralidade da Rede. A censura na Internet ocorre, por exemplo, quando usuários têm seu acesso bloqueado a determinadas páginas Web ou serviços. Existem diversas soluções para detecção de censura (SFAKIANAKIS; ATHANASOPOULOS; IOANNIDIS, 2011; NET..., 2015a; HWANG, 2007; BASSO;

FILASTÒ, 2015; FILASTÒ; APPELBAUM, 2012). Estas soluções monitoram a rede efetuando medições periodicamente, criando assim um "censo" sobre assuntos, serviços e páginas Web bloqueados e/ou filtrados. Um survey bastante completo sobre detecção de censura na Internet foi publicado recentemente e foi descrito na Seção 2.3 desta tese (ACETO; PESCAPÉ, 2015).

Um tema relacionado à censura é a modificação de conteúdo. Exemplos desta prática incluem: alterar o conteúdo de uma página Web (inserindo anúncios, por exemplo), injetar pacotes forjados em um fluxo de comunicação ou ainda modificar o conteúdo dos pacotes (prejudicando a integridade dos dados transferidos por BitTorrent, por exemplo). Existem algumas soluções para detectar estes tipos de práticas. A Switzerland (SWITZERLAND..., 2015) é uma ferramenta para a detecção de modificação e injeção de pacotes de dados trafegando na Internet. Já em (REIS et al, 2008) os autores apresentam uma solução para detectar modificações feitas em páginas Web no caminho entre o servidor e o usuário final, como inserção de anúncios e códigos maliciosos, por exemplo.

Diversos trabalhos sobre medições de rede podem ser utilizados no contexto da Neutralidade da Rede. Os dados coletados por plataformas e serviços de medição (DHAWAN et al., 2012; DISCHINGER et al., 2007; MAHAJAN et al., 2008; BISCHOF et al., 2011; DOVROLIS et al., 2010) podem ser utilizados para detecção de violações da Neutralidade da Rede. Estas soluções monitoram continuamente diversas propriedades da rede de diversos ISPs, possibilitando também uma comparação de desempenho entre ISPs distintos. Um survey completo sobre plataformas de medição na Internet foi publicado recentemente e consta da Seção 2.3 desta tese (BAJPAI; SCHÖNWÄLDER, 2015). Diversas técnicas para medição de rede e geração de tráfego (VISHWANATH; VAHDAT, 2009; MICHAUT; LEPAGE, 2005; BASSO; MEO; DE MARTIN, 2013; KANUPARTHY; DOVROLIS, 2011; CHENG et al., 2004; BOTTA; DAINOTTI; PESCAPÉ, 2012) também podem ser utilizadas na detecção de diferenciação (empregando tipos diferentes de tráfego) e para medir qualidade de serviço de ISPs. São descritos abaixo alguns trabalhos sobre medição de rede, diretamente voltados para a obtenção de dados que podem ser utilizados na detecção de algum tipo de violação da Neutralidade da Rede.

A Neubot (Network Neutrality Bot) (MARTIN; GLORIOSO, 2008; BASSO; SERVETTI; DE MARTIN, 2011) é uma plataforma de software para a obtenção contínua de medições distribuídas na Internet. A Neubot permite a implementação de

ferramentas e estratégias para verificar a qualidade do serviço oferecido por ISPs, conforme diferentes protocolos e/ou aplicações são utilizados nas medições. As medições implementadas na Neubot são executadas periodicamente em hosts finais e todos os dados obtidos são disponibilizados publicamente. As medições de rede já implementadas pela Neubot incluem os protocolos HTTP, BitTorrent, RTP, VoIP, entre outros. Porém, a Neubot não implementa nenhuma detecção de violações da Neutralidade da Rede, servindo apenas para obtenção de medições que poderão ser utilizadas para tal. Desde fevereiro de 2012 a Neubot efetua suas medições dentro da plataforma de medição Measurement Lab (DOVROLIS et al., 2010), utilizando os diversos servidores de medição disponibilizados pela plataforma. Os autores afirmam que a grande quantidade de dados de medição referentes à qualidade da Internet de usuários finais permite uma análise sistemática dos serviços de Internet sendo oferecidos pelos ISPs. Os autores afirmam ainda que os dados coletados pela Neubot podem trazer um melhor entendimento da Neutralidade da Rede baseado em dados reais, contribuindo assim com o atual debate mundial.

O Netalyzr (KREIBICH et al., 2010) é um serviço de medição de rede cujo objetivo é avaliar a conexão de Internet de usuários finais, coletando dados que podem ser utilizados para identificar violações da Neutralidade da Rede e problemas de rede. O projeto do Netalyzr visa abranger a maior quantidade possível de métricas e ser de fácil utilização por usuários sem conhecimento técnico. O Netalyzr é implementado como um applet Java (executado em um navegador) que se comunica com diversos servidores de medição. São efetuadas diversas medições referentes a diversos protocolos (como TCP, UDP, HTTP e DNS), à rede local do usuário (como NAT e buffers), ao ISP de acesso (como suporte IPv6, modificação de conteúdo, filtragem de portas, largura de banda e latência), entre outras. Além de informar as medições ao usuário, a ferramenta também funciona como um serviço de monitoramento contínuo de hosts na borda da Internet, já que armazena todas as medições feitas pelos diversos usuários finais na Internet. Assim, tem-se uma grande base de dados que pode ser utilizada para a detecção de diversas características da rede, inclusive para estudos referentes à Neutralidade da Rede. Os autores apresentam uma análise sobre 130.000 medições registradas pelo Netalyzr, as quais foram disponibilizadas publicamente.

A NNMA (NNSquad Network Measurement Agent) (NNSQUAD, 2015) é uma ferramenta que monitora a atividade de rede dos hosts em que está instalada. Este monitoramento tem como objetivo obter diversas medições de rede que possam

posteriormente auxiliar na detecção de violações da Neutralidade da Rede e problemas na rede. No contexto de Neutralidade da Rede, a principal medição feita pela NNMA é a identificação de pacotes forjados do tipo RST (reset) do protocolo TCP. Um pacote RST indica que um dos hosts encerrou a conexão e não irá mais enviar ou receber pacotes. ISPs podem injetar pacotes RST forjados para encerrar conexões referentes a algum tipo de tráfego específico (WEAVER; SOMMER; PAXSON, 2009). A NNMA não efetua nenhuma comparação sobre a quantidade de pacotes RST forjados para o tráfego de diferentes aplicações. Porém, é uma métrica que pode ser utilizada para inferir se um ISP está efetuando diferenciação de tráfego utilizando tal prática.

4.3. CONSIDERAÇÕES FINAIS

O número de ferramentas apresentadas e a diversidade nas formas de detecção de violações da Neutralidade da Rede confirmam a importância do tema e a sua atualidade. Confirmam também o envolvimento da comunidade técnico-científica no debate da Neutralidade da Rede. São os membros desta comunidade que, atentos ao debate teórico, por meio das ferramentas buscam garantir na prática, a detecção da efetividade da aplicação do que foi estabelecido na normatização para uma rede neutra, ou a detecção da sua violação de alguma forma. As ferramentas de monitoramento da Neutralidade da Rede aqui apresentadas baseiam-se, em geral, em medições de rede e métodos estatísticos para inferir se um ISP está discriminando um tipo de tráfego de dados em relação a outros. Estas ferramentas diferem, principalmente, na topologia utilizada para medição, nas métricas empregadas, no tipo de comparação estatística realizada e nos requisitos e limitações das estratégias adotadas. Foram apresentadas aqui também outras ferramentas relacionadas à Neutralidade da Rede que não se referem diretamente à detecção de diferenciação de tráfego. Estes outros trabalhos tratam de outros tipos de violação da Neutralidade da Rede, como censura ou qualidade de serviço inferior à contratada, por exemplo, além de outras soluções que podem ser utilizadas no contexto da Neutralidade da Rede.

Em face ao exposto neste capítulo, é possível inferir que não obstante diversos países tenham instituído regras para uma rede neutra, fiscalizar se a Neutralidade da Rede está sendo cumprida pelos ISPs ainda é um desafio. Além disso, não obstante a existência de ferramentas projetadas para monitorar tanto redes fixas como móveis, há

ferramentas projetadas de maneira específica para monitorar somente redes móveis. Diante disso, é possível inferir também que há um movimento claro que visa garantir a neutralidade de redes móveis. E, ainda, não obstante tenham sido apresentadas ferramentas com variadas formas de monitoramento para detecção de alguma violação no contexto da Neutralidade da Rede, é possível inferir que o monitoramento do tráfego da Internet representa o maior desafio. Esta inferência leva em conta a complexidade da estrutura das redes *versu*s a complexidade de projetar as funcionalidades necessárias a uma ferramenta que contemple todas as variáveis possíveis do gerenciamento de tráfego, a fim de comprovar alguma manipulação indevida. E, de modo análogo, esta inferência leva em conta a dinâmica do debate da Neutralidade da Rede, na qual os agentes envolvidos, em especial os ISPs, atuam de modo a adaptar seu gerenciamento de tráfego e o seu modelo de negócios a fim de dificultar a comprovação da violação à Neutralidade da Rede que porventura estejam efetuando.

CAPÍTULO V

CRIAÇÃO DO OBSERVATÓRIO DA NEUTRALIDADE DA REDE

Este capítulo tem por objetivo apresentar o panorama da Internet no Brasil e, neste contexto, criar o observatório da Neutralidade da Rede. Para atingir o objetivo proposto, este capítulo é dividido da seguinte maneira. A Seção 5.1 apresenta o panorama da Internet no Brasil, e a Seção 5.2 apresenta o observatório nacional da Neutralidade da Rede. Para mostrar o panorama da Internet no Brasil, a Seção 5.1 é subdividida da seguinte forma. Na Subseção 5.1.1 é apresentado o papel de cada agente envolvido no debate da Neutralidade da Rede no Brasil e na Subseção 5.1.2 são mostradas as ferramentas computacionais, que possuem alguma relação com a Neutralidade da Rede, e que estão disponíveis no Brasil para os usuários. Já na Subseção 5.1.3 é exposta a figura do Panorama da Internet no Brasil e na Subseção 5.1.4 são apresentadas as considerações finais a esta seção. Importante ressaltar que a normatização da Neutralidade da Rede no Brasil não é apresentada neste panorama brasileiro, considerando que já foi apresentada no Capítulo 3, que tratou do Panorama Mundial da Normatização da Neutralidade da Rede.

Para situar o papel de cada agente brasileiro envolvido no debate, a Subseção 5.1.1 está subdivida em 12 itens da seguinte maneira. O item 5.1.1.1 trata da Agência Nacional de Telecomunicações (Anatel). O item 5.1.1.2 trata do Conselho Administrativo de Defesa Econômica (CADE). O item 5.1.1.3 trata da Secretaria Nacional do Consumidor (Senacon). O item 5.1.1.4 trata do Instituto Brasileiro de Defesa do Consumidor (Idec). O item 5.1.1.5 trata da PROTESTE. O item 5.1.1.6 trata do Ministério Público Federal (MPF). O item 5.1.1.7 trata do Comitê Gestor da Internet no Brasil (CGI.br) e do Núcleo de Informação e Coordenação do Ponto BR (NIC.br). O item 5.1.1.8 trata da Associação Brasileira de Telecomunicações (TELEBRASIL). O item 5.1.1.9 trata da Associação Brasileira de Internet (ABRANET). O item 5.1.1.10 trata da Associação Brasileira de Provedores de Internet e Telecomunicações (Abrint).

O item 5.1.1.11 trata dos Provedores de Serviços de Internet (ISPs). O item 5.1.1.12 trata da Rede Nacional de Ensino e Pesquisa (RNP).

Para revelar as ferramentas computacionais disponíveis no Brasil, a Subseção 5.1.2 está subdivida em 5 itens da seguinte maneira. O item 5.1.2.1 exibe o Sistema de Medição de Tráfego Internet (SIMET), que inclui as ferramentas SIMET Box; SIMET Web; SIMET Mobile e Monitor Banda Larga. O item 5.1.2.2 exibe as ferramentas Whitebox e Entidade Aferidora da Qualidade (EAQ). O item 5.1.2.3 exibe a ferramenta SpeedTeste. O item 5.1.2.4 exibe a ferramenta MinhaConexao. O item 5.1.2.5 exibe a ferramenta TESTE COPEL.

Para criar o Observatório Nacional da Neutralidade da Rede (ONR), a Subseção 5.2 está subdivida em 5 itens da seguinte maneira. O item 5.2.1 traz a justificativa para a criação do ONR. O item 5.2.2 traz a missão e os valores do ONR. O item 5.2.3 traz o objetivo e as atribuições do ONR. O item 5.2.4 revela a arquitetura do ONR. E, finalmente, o item 5.2.5 traz as considerações finais a esta seção.

5.1 O PANORAMA DA INTERNET NO BRASIL

Esta seção tem por objetivo estampar o panorama atual da Internet no Brasil, revelando os vários agentes envolvidos no debate da Neutralidade da Rede, o papel de cada um e, em especial, visa descortinar a maneira como estes agentes se inter-relacionam. Para tanto, foi elaborada a figura do panorama nacional da Internet, apresentada e comentada ao final da seção.

5.1.1 O Papel de Cada Agente Envolvido no Debate

Esta Subseção se propõe a levantar e listar cada um dos principais agentes envolvidos com a Internet no Brasil e, consequentemente, no debate da Neutralidade da Rede, situando assim cada agente e o seu papel, no panorama atual brasileiro.

5.1.1.1 A Agência Nacional de Telecomunicações (Anatel)

A Anatel foi criada pela Lei 9.472, de 16 de julho de 1997 (BRASIL, 1997b). De acordo com esta Lei, a Anatel é uma entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial e vinculada ao Ministério das Comunicações. A Anatel é administrativamente independente, é financeiramente autônoma e sem subordinação hierárquica.

A Anatel (ANATEL, 2015a) foi a primeira agência reguladora a ser instalada no Brasil. Isto se deve à Emenda Constitucional n°8/1995 (BRASIL, 1995), que eliminou a exclusividade da concessão para exploração de serviços de telecomunicações a empresas sob controle acionário estatal. Com essa alteração da Constituição, o Estado passou da função de provedor para a de regulador dos serviços de telecomunicações.

Cabe à Anatel (ANATEL, 2015a) adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações no Brasil, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade. A Anatel é sediada em Brasília e realiza as atividades de fiscalização por meio de Gerências Regionais e Unidades Operacionais, instaladas em todas as capitais brasileiras. A sua missão é regular o setor de telecomunicações para contribuir com o desenvolvimento do Brasil. Seu objetivo é promover o desenvolvimento das telecomunicações do país de modo a dotá-lo de uma moderna e eficiente infraestrutura de telecomunicações, capaz de oferecer à sociedade serviços adequados, diversificados e a preços justos, em todo o território nacional.

No rol de atribuições desta Agência destacam-se: (i) implementar, em sua esfera de atribuições, a política nacional de telecomunicações; (ii) reprimir infrações aos direitos dos usuários; e (iii) exercer, relativamente às telecomunicações, as competências legais em matéria de controle, prevenção e repressão das infrações da ordem econômica, ressalvadas as pertencentes ao Conselho Administrativo de Defesa Econômica (Cade) (ANATEL, 2015a).

A partir de janeiro de 2014 a Anatel (ANATEL, 2014) lança o espaço do consumidor em seu *site* para que ele possa efetuar reclamação, denúncia ou pedido de informação sobre a sua operadora de telecomunicações. A partir do dia primeiro de novembro de 2014 (ANATEL..., 2014), a Anatel aumentou o rigor na fiscalização das operadoras de banda larga. As prestadoras devem garantir mensalmente, em média, 80% da velocidade contratada pelos usuários. De acordo com as metas estabelecidas nos regulamentos de Gestão da Qualidade dos Serviços de Comunicação Multimídia (banda

larga fixa), e Móvel Pessoal (banda larga móvel), da Anatel, as prestadoras deverão garantir mensalmente, em média, 80% da velocidade contratada pelos usuários.

Diante disso, na prática, na contratação, por exemplo, de um plano de 10 MBps, a média mensal de velocidade deve ser de, no mínimo, 8 MBps. A velocidade instantânea, aquela aferida pontualmente em uma medição, deve ser de no mínimo 40% do contratado, ou seja, 4 MBps. Com isso, caso a prestadora entregue apenas 40% da velocidade contratada por vários dias, terá de, no restante do mês, entregar uma velocidade alta ao usuário para atingir a meta mensal de 80%.

5.1.1.2 O Conselho Administrativo de Defesa Econômica (CADE)

O CADE (CADE, [2017]) foi criado pela já revogada Lei n° 4.137/62, para fiscalizar a gestão econômica e o regime de contabilidade das empresas. Em junho de 1994, este órgão foi transformado em uma autarquia vinculada ao Ministério da Justiça pela Lei n° 8.884 (BRASIL, 1994), tendo sua sede e foro no Distrito Federal, e com jurisdição em todo o Território nacional. Em 2011, suas atribuições foram estabelecidas pela Lei nº 12.529 (BRASIL, 2011c), quando passou então a ser responsável por instruir os processos administrativos de apuração de infrações à ordem econômica. Ao CADE (MJC, 2017) compete prevenir e reprimir as infrações contra a ordem econômica, orientado pelos ditames constitucionais de liberdade de iniciativa, livre concorrência, função social da propriedade, defesa dos consumidores e repressão ao abuso do poder econômico.

O CADE tem como missão zelar pela livre concorrência no mercado, sendo responsável, no âmbito do Poder Executivo, não só por investigar e decidir, em última instância, sobre a matéria concorrencial, como também fomentar e disseminar a cultura da livre concorrência. Embora o CADE seja uma autarquia em regime especial, ele não é uma agência reguladora da concorrência, e sim uma autoridade de defesa da concorrência. Sua responsabilidade é julgar e punir administrativamente, em instância única, pessoas físicas e jurídicas que pratiquem infrações à ordem econômica, não havendo recurso para outro órgão.

Além disso, o Conselho também analisa atos de concentração, de modo a minimizar possíveis efeitos negativos no ambiente concorrencial de determinado mercado. Não estão entre as atribuições da autarquia regular preços e analisar os

aspectos criminais das condutas que investiga. Suas competências também não se confundem, por exemplo, com as de órgãos e entidades de defesa do consumidor, como o Procon (dos Estados e Municípios), e como a Secretaria Nacional do Consumidor (CADE, [2017]).

O papel do CADE de prevenir e reprimir as infrações contra a ordem econômica inclui a Internet, e especificamente quanto à Neutralidade da Rede, o relatório de gestão do CADE, de 2015 (CADE, 2016) traz que o Departamento de Estudos Econômicos do CADE realizou quatro edições do projeto Seminários Economia e Defesa da Concorrência, sendo que uma destas quatro edições teve como tema a Neutralidade da Rede, expondo uma análise sobre o mercado de dois lados, e na qual questiona a provável necessidade da atuação do CADE para resolver questões de discriminação e priorização de tráfego, e também se o CADE ficará na posição de preencher as eventuais lacunas da regulação (BRITTO, 2015).

5.1.1.3. A Secretaria Nacional do Consumidor (Senacon)

A Senacon, criada pelo Decreto nº 7.738, de 28 de maio de 2012 (BRASIL, 2012), integra o Ministério da Justiça e tem suas atribuições estabelecidas no art. 106 do Código de Defesa do Consumidor (BRASIL, 1990) e no art. 3º do Decreto n° 2.181/97 (BRASIL, 1997a).

A atuação da Senacon (SENACON, 2017) concentra-se no planejamento, elaboração, coordenação e execução da Política Nacional das Relações de Consumo. Dentre os objetivos da Senacon estão: (i) garantir a proteção e exercício dos direitos dos consumidores; (ii) promover a harmonização nas relações de consumo; e (iii) incentivar a integração e a atuação conjunta dos membros do Sistema Nacional do Consumidor (SNDC) que congrega os Procons, o Ministério Público, a Defensoria Pública, as Delegacias de Defesa do Consumidor e as Organizações Civis de defesa do consumidor, que atuam de forma articulada e integrada com a Senacon.

A Senacon também atua na análise de questões que tenham repercussão nacional e interesse geral, na promoção e coordenação de diálogos setoriais com fornecedores, na cooperação técnica com órgãos e agências reguladoras, na advocacia normativa de impacto para os consumidores, na prevenção e repressão de práticas infrativas aos direitos dos consumidores.

Dentre as principais ações da Senacon, destacam-se a articulação e integração dos órgãos que compõe o Sistema Nacional, por meio de reuniões ordinárias e grupos de trabalho, a prevenção e solução de conflitos de consumo por meio do Sistema Nacional de Informações de Defesa do Consumidor (Sindec) e a manutenção do *site consumidor.gov.br*, onde o consumidor pode se comunicar diretamente com empresas que participam voluntariamente e se comprometem a receber, analisar e responder as reclamações de seus consumidores em até 10 dias.

O *consumidor.gov.br* é um serviço público que permite a interlocução direta entre consumidores e empresas para solução de conflitos de consumo pela Internet. Monitorada pela Senacon, Procons, Defensorias, Ministérios Públicos e também por toda a sociedade, esta ferramenta possibilita a resolução de conflitos de consumo de forma rápida e desburocratizada.

O *consumidor.gov.br* permite relações entre consumidores, fornecedores e o Estado, considerando as seguintes premissas: (i) transparência e controle social são imprescindíveis à efetividade dos direitos dos consumidores; (ii) as informações apresentadas pelos cidadãos consumidores são estratégicas para gestão e execução de políticas públicas de defesa do consumidor; e (iii) o acesso a informação potencializa o poder de escolha dos consumidores e contribui para o aprimoramento das relações de consumo.

Por se tratar de um serviço provido e mantido pelo Estado, com ênfase na interatividade entre consumidores e fornecedores para redução de conflitos de consumo, a participação de empresas no *consumidor.gov.br*, só é permitida àqueles que aderem formalmente ao serviço, mediante assinatura de termo no qual se comprometem a analisar e investir todos os esforços disponíveis para a solução dos problemas apresentados. O consumidor, por sua vez, deve se identificar adequadamente e comprometer-se a apresentar todos os dados e informações relativas à reclamação relatada.

Dentre as operadoras de telecomunicações (Telefonia, Internet, TV por assinatura) que aderiram ao serviço *consumidor.gov.br*, estão: Claro Celular, Claro Fixo – Embratel, Claro TV, Copel Telecom, Intelig, NET, Nextel, Oi Celular, Oi Fixo, SKY, Tim, e Vivo - Telefônica (GVT) (SENACON, 2017).

5.1.1.4 O Instituto Brasileiro de Defesa do Consumidor (Idec)

O Idec (IDEC, 2017) é uma associação de consumidores fundada em 1987. Não possui fins lucrativos. É independente de empresas, governos ou partidos políticos. Os recursos financeiros para o desenvolvimento de suas atividades têm sua origem nas contribuições dadas pelos seus associados, na venda de assinaturas da Revista do Idec e outras publicações, além da realização de cursos. O Idec também desenvolve projetos que recebem recursos de organismos públicos e fundações independentes. Esse apoio não compromete a independência do Instituto. O Idec é membro pleno da *Consumers International*, uma federação que congrega mais de 250 associações de consumidores que operam no mundo todo.

A missão do Idec é promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica. O Idec tem como objetivos contribuir para: (i) que seja atingido o equilíbrio ético nas relações de consumo; (ii) a implementação e o aprimoramento da legislação de defesa do consumidor e de matérias correlatas; (iii) a repressão ao abuso do poder econômico nas relações de consumo e nas demais relações jurídicas correlatas; e (iv) a melhoria da qualidade de vida, especialmente no que diz respeito à melhoria da qualidade dos produtos e serviços.

Para o Idec, o conceito de consumidor não se restringe àqueles que participam do mercado, exercendo seu poder de compra, mas abrange também os que não conseguem acesso a bens e serviços essenciais, por falta de poder aquisitivo. O Idec publica notícias e demais informações para que os consumidores se previnam ou solucionem problemas relacionados ao consumo. Orienta e informa seus associados e os consumidores sobre seus direitos para que se previnam de problemas utilizando o Código de Defesa do Consumidor.

O Idec move ações judiciais coletivas em defesa do consumidor. Sejam ações contra empresas ou governos, nas quais os beneficiários são seus associados como um todo, ou grupo de associados. O Idec move também ações civis públicas que beneficiam todos os consumidores, toda a sociedade. O Idec não promove processos que tenham interesse apenas individual. O *site* do Idec traz várias matérias sobre os direitos dos consumidores relativos aos serviços de Internet e sobre as suas ações em defesa destes consumidores.

5.1.1.5 A PROTESTE

A PROTESTE (PROTESTE, 2017) é a Associação Brasileira de Defesa do Consumidor. É uma entidade civil sem fins lucrativos, apartidária, independente de governos e empresas, que atua na defesa e no fortalecimento dos direitos dos consumidores brasileiros. A PROTESTE foi fundada em 16 de julho de 2001, e é mantida com as mensalidades de seus associados e com o aporte e a solidariedade de outras associações de consumidores internacionais. A PROTESTE ajuda os cidadãos a conhecer seus direitos e também se mobiliza para aperfeiçoar a legislação de consumo. A PROTESTE intervém, sempre que necessário, nos conflitos de associados com fornecedores e encaminha às empresas e às autoridades reivindicações e propostas pertinentes para melhorar produtos e serviços.

A missão da PROTESTE é: promover a defesa dos consumidores e cidadãos; prover a melhor decisão de compra para o associado; e contribuir para melhorar as relações de consumo na sociedade. Os valores da PROTESTE são: (i) independência; (ii) proximidade; e (iii) excelência.

Em março de 2015 a PROTESTE realizou uma campanha chamada Teste sua Conexão (PROTESTE, 2015). O medidor de velocidade de Internet foi lançado em parceria com o *site* MinhaConexão (exposto nesta tese no item 5.1.2.4), para estimular o internauta a fazer medições ao longo do mês. A PROTESTE realizou esta campanha com o intuito de ajudar o consumidor a buscar os seus direitos nos casos de constatação de descumprimentos ao contrato com a sua operadora.

Mais da metade dos consumidores que utilizaram o medidor da PROTESTE, para monitorar a taxa recebida da sua operadora de Internet, aferiram velocidade abaixo da contratada. Até o dia 30 de março, 128 mil usuários haviam se cadastrado e 5 mil haviam respondido a pesquisa. Dos que afirmaram que a taxa média de velocidade recebida era inferior à contratada, 19% apontaram diferença de 10% a menos. E 14% dos entrevistados detectaram nas medições uma taxa de velocidade 50% menor do que a contratada (PROTESTE, 2015).

5.1.1.6 O Ministério Público Federal (MPF)

O MPF (MPF, 2017) integra o Ministério Público brasileiro, estabelecido na Constituição Federal de 1988 (BRASIL, 1988). De acordo com a Constituição Federal (BRASIL, 1988), cabe ao Ministério Público brasileiro: (i) a defesa dos direitos sociais e individuais indisponíveis; (ii) a defesa da ordem jurídica; e (iii) a defesa do regime democrático. O Ministério Público brasileiro é composto pelos Ministérios Públicos nos estados e pelo Ministério Público da União (MPU).

Os Ministérios Públicos nos estados atuam na Justiça estadual, enquanto que o MPF atua na Justiça Federal, em causas nas quais a Constituição considera haver interesse federal. A atuação pode ser judicial como fiscal da lei, cível e criminal, mas também pode ser extrajudicial, quando promove acordos por meio determos de ajuste de conduta, recomendações, inquérito civil público e audiências públicas. O MPU possui quatro ramos: o Ministério Público Federal (MPF), o Ministério Público do Trabalho (MPT), o Ministério Público Militar (MPM) e o Ministério Público do Distrito Federal e Territórios (MPDFT) (BRASIL, 1988). O ramo do MPU de interesse para esta tese recai, assim, sobre o MPF, pela sua maior aderência ao tema aqui tratado.

Também de acordo com a Constituição Brasileira de 1988 (BRASIL, 1988) o MPF foi instituído como instituição independente, extra poder, dotada de independência funcional, administrativa e financeira, com a função de zelar pelo efetivo respeito dos poderes públicos e dos serviços de relevância pública aos direitos assegurados na Constituição, promovendo as medidas necessárias a sua garantia. O MPF tem por missão promover a realização da Justiça, a bem da sociedade e em defesa do estado democrático de direito. Cabe ao MPF assegurar o respeito aos direitos dos cidadãos, por meio da fiscalização e cobrança na aplicação das leis.

O MPF, assim como o Ministério Público brasileiro, não faz parte de nenhum dos três poderes (Executivo, Legislativo e Judiciário) e tem independência funcional assegurada pela Constituição Federal. O MPF atua em casos federais, regulamentados pela Constituição e pelas leis federais, sempre que a questão envolver interesse público. O chefe do MPF é o procurador-geral da República, nomeado pelo presidente da República, com autorização da maioria absoluta do Senado Federal, e a sede administrativa do MPF é a Procuradoria-Geral da República.

A defesa da legislação referente à Internet também está a cargo do MPF, sendo um exemplo disso a Nota Técnica Nº 02/2015, do MPF, que analisou o Projeto Internet.org do Facebook e o princípio da Neutralidade da Rede, divulgada em 11 de novembro de 2015, e relatado à página 57 desta tese.

5.1.1.7 O Comitê Gestor da Internet no Brasil (CGI.br)

O CGI.br (CGI, 2017) foi criado pelo Decreto Nº 4.829, de 3 de setembro de 2003 (BRASIL, 2003). De acordo com este Decreto, dentre as atribuições do CGI.br, estão: (i) estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil; (ii) estabelecer diretrizes para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (*Internet Protocol*) e na administração pertinente ao Domínio de Primeiro Nível (ccTLD - *country code Top Level Domain*) ".br", no interesse do desenvolvimento da Internet no País; (iii) propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados; (iv) promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade; (v) articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet; (vi) adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere; e (vii) deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País.

O CGI.br (CGI, 2017) também promove estudos e recomenda procedimentos para a segurança da Internet e ainda propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da Internet. Em resumo, o CGI.br é o órgão responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

5.1.1.7.1 O Núcleo de Informação e Coordenação do Ponto BR (NIC.br)

O NIC.br (NIC.BR, 2017) é uma entidade civil, de direito privado e sem fins lucrativos , que foi criado para implementar as decisões e os projetos do CGI.br sendo, portanto, considerado seu braço executivo. Em 2003 o NIC.br foi formalmente estabelecido como pessoa jurídica. Em 2005, o NIC.br passou então a ser a instituição que administra as ações de registro de nomes sob o .br, além de assumir outras atribuições.

Dentre as atribuições e/ou atividades permanentes do NIC.br estão: (i) coordenar o registro de nomes de domínio, o Registro.br (REGISTRO, 2017); (ii) estudar, responder e tratar incidentes de segurança no Brasil, por meio do CERT.br (CERT, 2017); (iii) estudar e pesquisar tecnologias de redes e operações, por meio do Ceptro.br (CEPTRO, 2017); (iv) produzir indicadores sobre as tecnologias da informação e da comunicação, por meio do Cetic.br (CETIC, 2017); (v) implementar e operar os Pontos de Troca de Tráfego, por meio do IX.br (IX.BR, 2017); (vi) viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas, por meio do Ceweb.br (CEWEB, 2017); (vi) abrigar o escritório do W3C no Brasil (W3C BRASIL, 2017) que promove ações para o desenvolvimento e fortalecimento dos padrões Web; e (vii) promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.

Estas atividades são mantidas com a arrecadação de recursos que ocorre por meio do registro de domínios ".br" e a alocação de endereços IP. Estas ações são conduzidas pelo NIC.br de forma autônoma e privada, sem aporte de recursos públicos. Diferentemente do que acontece com outros NICs existentes no mundo, além de proporcionar e manter alta qualidade na atividade de registro de domínios, o montante arrecado exclusivamente pelo Registro.br é investido em ações e projetos que geram benefícios e a melhoria das atividades relacionadas à infraestrutura da Internet disponíveis no País.

5.1.1.8 A Associação Brasileira de Telecomunicações (TELEBRASIL)

A TELEBRASIL (TELEBRASIL, 2017) é uma entidade civil, de caráter privativo e âmbito nacional, sem finalidade lucrativa, que congrega operadores e fornecedores de bens e serviços do setor de comunicações e informação para a defesa de

seus interesses e desenvolvimento. Funciona como um portal de entrada para as empresas interessadas em negócios de telecomunicações e um canal institucional de acesso aos órgãos governamentais, como o Ministério das Comunicações, a Anatel e a Comissão de Ciência e Tecnologia da Câmara dos Deputados.

Podem ser associadas da TELEBRASIL as pessoas jurídicas de direito público ou privado cujas atividades estejam, no todo ou em parte, voltadas para as telecomunicações, seja como geradores ou usuários de serviços ou produtos deste setor, assim como também outras instituições e pessoas interessadas no fomento desta atividade. Dentre os associados à TELEBRASIL encontram-se: a Associação Brasileira de Internet e várias operadoras tais como Oi, Telefónica, Tim, Vivo e Claro.

5.1.1.9 A Associação Brasileira de Internet (ABRANET)

De acordo com a Abranet (ABRANET, 2017), a sua história se confunde com a história da Internet no Brasil. Fundada em 7 de novembro de 1996, a Abranet é uma associação civil, sem fins lucrativos. É uma organização não governamental, inicialmente designada como Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet. Em 8 de maio de 2009 o seu estatuto foi atualizado (ABRANET, 2009), passando a se chamar então Associação Brasileira de Internet, abrangendo de forma mais ampla toda a cadeia da Internet no Brasil.

A Abranet tem como principal objetivo social o apoio às empresas que ofertam serviços, informações, realizam pesquisa e desenvolvimento e as demais atividades profissionais e acadêmicas relacionadas com a tecnologia da informação e Comunicação e a Internet no país. A Abranet Conhece profundamente os desafios dos provedores e sabe como intervir a favor deles nas discussões que ditam os rumos da internet no País. Trabalha para garantir a sustentabilidade do setor, provendo as empresas de ferramentas e informações relevantes que otimizam a gestão dos negócios.

Dentre as atividades da Abranet cabe destacar: (i) a promoção da conscientização da sociedade para a importância da liberdade de expressão e livre fluxo internacional de informações na Internet como base para o desenvolvimento econômico e social das pessoas e entidades nacionais promovendo a difusão e utilização da Internet nas mais diversas aplicações sociais, industriais, comerciais, de serviços, científicas e culturais; (ii) a promoção e estímulo ao desenvolvimento e intercambio de informações

sobre tecnologias de comunicação e informação, inclusive sobre técnicas e tecnologias utilizadas na Internet; (iii) a participação ativa na articulação dos vários segmentos da sociedade, tendo como objetivo estimular a inovação, a liberdade de expressão, o fluxo de informações livre e ilimitado tanto no contexto nacional como internacional para o desenvolvimento contínuo da Internet no Brasil; e (iv) a participação ativa na elaboração de políticas públicas, e do arcabouço legal relativo ao uso da Internet, apresentando às autoridades governamentais e demais entidades competentes, estudos, sugestões e críticas, visando, em especial: a) o desenvolvimento e fortalecimento da Internet no Brasil, observando os valores e princípios fundamentais dos direitos humanos estabelecidos pelas Nações Unidas; b) o desenvolvimento e fortalecimento da infraestrutura nacional e internacional para assegurar a conectividade na Internet com qualidade e custos razoáveis e compatíveis com os usos e aplicações demandados pelas pessoas e empresas e difundidos em âmbito mundial; c) promover a cooperação entre seus associados, visando a disseminação de boas práticas e de conhecimentos e inovação para desenvolvimento das tecnologias de comunicação e informação e da Internet no país; d) promover no seu âmbito de atuação, condições de livre concorrência e isonomia entre os participantes da Internet, em especial no acesso isonômico e não discriminatório a recursos, serviços e informações; e e) promover a realização de atividades de pesquisa e desenvolvimento para inovação das tecnologias de comunicação e informação e da Internet.

5.1.1.10 A Associação Brasileira de Provedores de Internet e Telecomunicações (ABRINT)

A ABRINT (ABRINT, 2017) é uma associação civil, de fins não econômicos, que tem como objetivo a representatividade de seus associados junto à sociedade, ao governo e aos órgãos reguladores nos assuntos pertinentes ao setor. Os associados da ABRINT estão em todos os estados brasileiros e representam empresas de provimento de acesso à Internet. Os provedores regionais de Internet têm na ABRINT a representação institucional e política, necessárias à garantia de um ambiente competitivo saudável e à consequente ampliação da oferta de serviços e crescimento dos seus negócios.

A ABRINT tem como objetivos o apoio e defesa dos interesses das empresas provedoras de serviços de Internet e telecomunicações, visando à promoção e desenvolvimento da Rede Internet no Brasil. Dentre as atribuições da ABRINT estão: (i) promover a conscientização da comunidade para a importância econômica e social das atividades na Internet, promovendo sua difusão e utilização em aplicações industriais, comerciais, prestação de serviços, científicas, culturais e outras correlatas; (ii) promover a congregação dos provedores de serviços e informações da Internet, assim como dos produtores de serviços afins, para a defesa de seus interesses; (iii) participar de forma ativa, encaminhando às autoridades governamentais e demais entidades competentes estudos e sugestões visando o desenvolvimento e fortalecimento do mercado da Internet; (iv) participar, junto aos órgãos governamentais e às autoridades, dos debates para a definição das políticas que permitam garantir uma infraestrutura de conectividade de alta qualidade e compatível com os padrões tecnológicos mundiais, procurando ter lugar e voto nos órgãos que existirem e/ou nos que vierem a ser constituídos com essa finalidade; (v) participar ativamente, em todas as esferas, pelo aprimoramento da legislação e da regulamentação relativa às atividades na Internet em geral; (vi) desenvolver e editar um código de ética estabelecendo padrões de conduta para o setor; (vii) representar os associados em processos de interesse comum, judicial ou extrajudicialmente, nos termos do artigo 5º, inciso XXI, da Constituição Federativa do Brasil de 1988, em todas as instâncias do poder judiciário, podendo para tanto praticar atos em nome dos associados, inclusive atuar em substituição em ações judiciais, desde que aprovada pela diretoria executiva da ABRINT; (viii) impetrar mandado de segurança coletivo em defesa dos interesses de seus associados, total ou parcialmente, nos termos do Art. 5º., inciso LXX, alínea “b” da Constituição Federal; e (ix) defender os interesses dos associados, proporcionando-lhes assistência por todos os meios ao seu alcance dentro dos objetivos da ABRINT.

5.1.1.11 Os Provedores de Serviços de Internet (ISPs)

De acordo com o exposto no Panorama setorial da Internet, do Nic.br (PANORAMA..., 2016), os ISPs são atores fundamentais para o funcionamento da Internet no Brasil e no mundo. O setor de provimento desempenha um papel relevante tanto para a ampliação da oferta de acesso à rede quanto no provimento de serviços de

acesso de qualidade. À medida que operam e mantêm uma parte crítica da infraestrutura de Internet, consolidam-se como um meio crucial para garantir a conectividade entre pessoas, organizações, governos e todos os participantes da rede mundial de computadores.

O setor de ISPs é formado por um grupo de empresas que presta uma diversificada gama de serviços de Internet. As categorias desse grupo vão desde os provedores de backbone até os provedores de conteúdo, passando pelos provedores de acesso, provedores de hospedagem, entre outros. Os serviços de provimento de acesso à Internet, particularmente, representam o tipo de serviço mais ofertado (PANORAMA..., 2016).

Para o CGI.br, em sua pesquisa TIC Provedores 2014 (CGI, 2016b), os provedores de serviços de Internet são todas as empresas que atuam em território nacional oferecendo os serviços de Internet, que incluem: provimento de acesso, conteúdo, hospedagem, e-mail ou aplicações. Nesta pesquisa foram identificados 2.138 ISPs atuando nesse mercado no Brasil em 2014. Destes 2.138 ISPs, 68% estão sediados nas regiões Sul e Sudeste, e apenas 5% estão sediados na região Norte. A maioria destes ISPs oferece seus serviços para o mercado privado (90%) e domiciliar (88%). Estas empresas atuam em menor escala no mercado público: 63% têm como clientes os governos municipais, 31% os governos estaduais e 21% o governo federal.

A *Tech in Brazil* (BOECHAT, 2015) publicou em novembro de 2015 uma lista com os maiores provedores de Internet disponíveis no Brasil, de acordo com a Anatel. Estes ISPs detêm em torno de 90% de todos os acessos no país, com cobertura nas principais capitais e regiões metropolitanas. São eles: Algar Telecom, Oi, Sky, Live TIM, Vivo, NET Virtua e GVT. O artigo traz também uma lista de provedores regionais, disponíveis em áreas que por vezes não estão cobertas pelos provedores maiores.

5.1.1.12 A Rede Nacional de Ensino e Pesquisa (RNP)

A RNP (RNP, 2017) foi criada em setembro de 1989 pelo Ministério da Ciência e Tecnologia (MCT). Seu objetivo era construir uma infraestrutura nacional de rede Internet de âmbito acadêmico. Em maio de 1995, teve início a abertura da Internet comercial no Brasil. Nesse período, a RNP passou por uma redefinição de seu papel,

estendendo seus serviços de acesso a todos os setores da sociedade. Com essa reorientação de foco, ofereceu um importante apoio à consolidação da Internet comercial no país. Nesta época foi criado o Centro de Informações da Internet Brasil, para dar suporte ao surgimento dos provedores e usuários da rede. Foi criado também o primeiro centro de segurança de redes brasileiro. Assim, diversas empresas fabricantes de bens de informática, tais como Compaq, Equitel, IBM, Philips, entre outras, passaram a oferecer apoio concreto à RNP, fornecendo equipamentos, software e, mesmo, financiando suas atividades diretas.

Em outubro de 1999, dez anos depois da criação do projeto RNP, os Ministérios da Ciência e Tecnologia (MCT) e da Educação (MEC) assinaram um convênio, o Programa Interministerial de Implantação e Manutenção da Rede Nacional para Ensino e Pesquisa (PI-MEC/MCT), hoje denominado Programa Interministerial RNP (PI-RNP). Estes dois ministérios investiriam, então, na implantação do backbone RNP2, a primeira infraestrutura de rede avançada, capaz de atender às novas necessidades de banda e de serviços para ensino e pesquisa. A Associação Rede Nacional de Ensino e Pesquisa (AsRNP), criada nesse mesmo ano pelos colaboradores do projeto RNP, apresentou-se para desenvolver e executar este programa, sob orientação de um Comitê Gestor (CG-RNP) formado por representantes do MEC e do MCT. O backbone RNP2 foi oficialmente inaugurado em maio de 2000.

A partir de 2002 a RNP passa a ser uma Organização Social (OS) vinculada ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC). A manutenção da RNP é feita por esse ministério em conjunto com os ministérios da Educação (MEC), Cultura (MinC), Saúde (MS) e Defesa (MD), representando o Estado brasileiro e, também, por universidades, sociedades científicas, usuários e associados, representando a sociedade civil.

Ainda que existissem iniciativas anteriores, de acordo com a RNP, ela começou em 2005 a construção das suas próprias redes metropolitanas, para prover acesso entre cada Ponto de Presença (PoP) e os campi das organizações usuárias na mesma cidade, por meio do projeto Redes Comunitárias de Ensino e Pesquisa (Redecomep). Essas redes metropolitanas permitem prover conexões de alta capacidade, tipicamente 1 ou 10 Gb/s, entre o PoP e o campus, utilizando uma infraestrutura de fibra óptica construída pela RNP. Em 2014, as redes já estavam em uso em quase 40 cidades do país.

A RNP está presente em todas as unidades da federação através de 27 Pontos de Presença, que formam a espinha dorsal da rede acadêmica nacional, a rede Ipê. Trata-se

de uma infraestrutura de rede óptica à qual estão conectados 1.522 campi e unidades nas capitais e no interior e por onde trocam grande volume de dados e informações em âmbito global. Essas organizações que compõem a RNP são as principais instituições de educação superior e produção de conhecimento e inovação do Brasil, abrangendo principalmente universidades, institutos e unidades de pesquisa federais e estaduais, hospitais de ensino e museus. A RNP promove e desenvolve parcerias públicas e privadas que viabilizam a superação de barreiras de infraestrutura, tecnologia e qualificação.

5.1.2 Ferramentas Computacionais

Esta subseção apresenta ferramentas computacionais disponibilizadas no Brasil, que se propõem a fornecer ao usuário da Internet, algum tipo de medição no tráfego que recebem.

5.1.2.1 Sistema de Medição de Tráfego Internet (SIMET)

O SIMET (SIMET, 2017) é um sistema que realiza testes de desempenho em redes com acesso a Internet, através de servidores espalhados dentro dos pontos de troca de tráfego Internet. O SIMET é 100% independente, ou seja, os testes são feitos fora das redes das operadoras, sempre que possível dentro dos PTTs do CGI.br. Todo desenvolvimento e infraestrutura do SIMET ficam a cargo do NIC.br. O SIMET disponibiliza um conjunto de ferramentas para fazer medições e testar a qualidade da rede: SIMET Box, SIMET Web, SIMET Mobile e o Monitor Banda Larga.

5.1.2.1.1 SIMET Box

O SIMET Box (SIMET BOX, 2017) é um medidor, disponibilizado por meio de um equipamento oferecido pelo NIC.br com o objetivo de analisar a qualidade da Internet automaticamente, várias vezes ao dia. Monitora a velocidade da conexão e realiza diversos testes adicionais. Além das funcionalidades básicas de um roteador,

com o SIMET Box é possível configurar rede doméstica Wi-Fi e redes WAN e LAN cabeadas, monitorar a velocidade da conexão e realizar diversos testes, tais como : (i) testes padrões do SIMET: vazão TCP e UDP, *jitter*, latência, perda de pacotes; (ii) teste de DNS: tempo de resposta, respeito ao campo TTL, validação de DNSSEC, suporte a IPv6, domínios inexistentes; (iii) gerência da porta 25: detecta a possibilidade de envio de *spam*; (iv) detecta a possibilidade de propagação de endereços de IP forjados; e (v) disponibilidade do acesso à Internet.

5.1.2.1.2 SIMET Web

O SIMET Web ((SIMET, 2017) mede a qualidade da Internet através do navegador do usuário: Google Chrome, Firefox, Internet Explorer ou Safari.

5.1.2.1.3 SIMET Mobile

O SIMET Mobile (SIMET MOBILE, 2017) é o Sistema de Medição de Tráfego da Internet para dispositivos móveis, ou seja, é um aplicativo que permite testar a qualidade da Internet. Com o SIMET Mobile é possível ao usuário: (i) saber qual a velocidade da sua Internet (*upload* e *download*) utilizando os protocolos TCP e UDP; (ii) saber a latência da sua rede; (iii) saber como está a qualidade da Internet em cada localidade testada; (iv) enviar os resultados encontrados via e-mail; e (v) compartilhar seus resultados em redes sociais.

O SIMET Mobile permite que o usuário saiba a qualidade da sua Internet utilizando tecnologias que impedem o seu provedor de mascarar os resultados. Os resultados do SIMET Mobile são utilizados pelo CGI.br para geração de um mapa da qualidade da Internet do Brasil. Todos os testes são feitos fora da rede da operadora do usuário. Este aplicativo é considerado pelo NIC.br como o primeiro voltado para usuários finais que realiza testes usando IPv6 no Brasil.

O aplicativo SIMET Mobile (APLICATIVO..., 2016) permite que os usuários testem o desempenho de redes de conexão 3G, 4G e Wi-Fi. Com isso, é possível usar o aplicativo para comparar a qualidade da conexão por operadoras e não por conjuntos totais de testes realizados. Outra funcionalidade é a possibilidade de medir a qualidade

do acesso à Internet por região. Para isso, o aplicativo leva em conta os resultados de testes feitos por outros usuários em diferentes tipos de atividades, incluindo acessar a web, fazer chamadas VoIP, assistir vídeos, entre outras. O aplicativo está disponível para aparelhos iOS e Android.

5.1.2.1.4 Monitor Banda Larga

O aplicativo Monitor Banda Larga (SIMET, 2017), foi desenvolvido pela FIESP (Federação das Indústrias do Estado de São Paulo), juntamente com seu parceiro tecnológico, o NIC.br. O Monitor Banda Larga é uma ferramenta que auxilia o usuário brasileiro de banda larga fixa a verificar, de maneira fácil e rápida, a qualidade e a velocidade de sua Internet.

A utilização do Monitor Banda Larga pelo usuário contribui para a avaliação da banda larga fixa de sua região e de seu provedor de acessos. O Monitor Banda Larga verifica critérios como a velocidade de *download* e *upload*, ou seja, a rapidez com que os dados dos usuários são enviados e recebidos pela Internet, além de outros parâmetros, emitindo um parecer sobre a adequação da sua conexão para as seguintes aplicações: (i) comunicação com voz via Internet; (ii) videoconferência; e (iii) jogos on-line.

O Monitor Banda Larga está disponível também para a rede móvel. O Monitor Banda Larga Móvel é compatível com os sistemas operacionais IOS e Android. Ao final da medição, o aplicativo mostra ao usuário a qualidade da sua Internet para: (i) acessar *site*s/redes; (ii) ligação com voz via Internet; (iii) videoconferência; e (iv) carregar vídeos. O Monitor Banda Larga Móvel também verifica a velocidade de *download* e *upload*. O tráfego dos pacotes é medido pelos parâmetros de latência e *jitter*.

Dentro do aplicativo o usuário também pode verificar o histórico dos resultados de suas medições, mapas de qualidade, resultados técnicos e detalhados dos parâmetros de qualidade medidos, além de poder compartilhar seus resultados em redes sociais. Com o aplicativo instalado em seu dispositivo, também é possível realizar testes em redes sem fio, caso esteja utilizando seus aparelhos conectados a redes Wi-Fi.

5.1.2.2 Whitebox e Entidade Aferidora da Qualidade (EAQ)

O Whitebox (WHITEBOX, 2015), da empresa SamKnows do Reino Unido, é um pequeno dispositivo de hardware baseado em Linux, capaz de executar um conjunto de medidas de desempenho em redes de banda larga. O Whitebox somente executa as medições quando o usuário não está usando sua conexão. A tecnologia SamKnows é incorporada diretamente ao ISP que a envia aos seus clientes. O teste é baseado na web e é capaz de medir *download*, *upload*, latência, perda de pacotes, além de *jitter*, com um alto grau de precisão. A SamKnows fornece também aplicativo de *smartphones* para medir o desempenho de banda larga móvel nas plataformas Android e iOS.

O Whitebox Mobile foi desenvolvido pela SamKnows em 2011 com o objetivo de medir o desempenho da Internet móvel em *dongles* (*modems* USB). Ele foi projetado para ser implantado de forma dedicada, com um ou mais USB *dongles*. Dentre os órgãos reguladores que utilizam a plataforma da SamKnows estão a FCC dos EUA, a Ofcom do Reino Unido, e a Anatel do Brasil. De acordo com a própria SamKnows (SAMKNOWS, 2015) ela trabalha no Brasil com a Anatel desde 2012, como parte da Entidade Aferidora da Qualidade (EAQ). A EAQ é uma parceria entre a SamKnows e a PricewaterhouseCoopers (PwC). O projeto utiliza a ferramenta Whitebox para medição em redes fixas e móveis. Os dados coletados são publicados pela Anatel e são usados para ajudar a reforçar as regulamentações de qualidade de serviço.

A PwC foi a empresa selecionada pela Anatel, em 2012, como EAQ no Brasil (ANATEL..., 2012), ficando responsável por analisar a qualidade do serviço de banda larga das operadoras brasileiras. Esta EAQ foi criada em atendimento à Resolução Anatel 574 (ANATEL, 2011a) e 575 (ANATEL, 2011b) de 28 de Outubro de 2011, como parte do processo de aferição dos indicadores de qualidade das redes de telecomunicações que suportam o acesso à Internet em Banda Larga fixa e móvel no Brasil.

De acordo com a ANATEL (ANATEL, 2015b) as versões oficiais dos aplicativos da Anatel para aferição da qualidade da banda larga móvel, para os sistemas operacionais iOS e Android, foram desenvolvidos pela EAQ. As ferramentas de medição permitem ao usuário, a qualquer tempo, medir a qualidade de sua conexão de banda larga Internet, fixa ou móvel, visualizando os resultados imediatamente, bem como o histórico das medições anteriores. Os resultados apresentados são medidas momentâneas da qualidade de conexão e indicam uma referência para o

acompanhamento do desempenho da rede. O Programa de Aferição de Qualidade da Banda Larga no Brasil da Anatel, no qual se insere a EAQ, visa medir os indicadores da qualidade e para isto conta com a participação de usuários que se inscrevem no programa como voluntários (ANATEL, 2017).

A decisão da Anatel em selecionar a empresa PWC, como EAQ, e a Samknows como a empresa parceira tecnológica da PWC, para dar o suporte técnico, gerou algumas críticas. De acordo com a Convergência Digital (GROSSMANN; QUEIROZ, 2012) a empresa PWC foi contratada pelas teles para atuar como EAQ em 2012. No ano anterior, em 2011, a PWC também foi contratada pelas operadoras para apresentar um estudo sobre os parâmetros então propostos pela Anatel e concluiu que tais critérios não tinham paralelo no planeta. E, no mesmo evento, promovido pelo sindicato das operadoras, a SamKnows apresentou suas experiências em medições de qualidade das conexões na Inglaterra e nos Estados Unidos. Os executivos da empresa vieram para oferecer seu sistema como uma alternativa. E, para os autores do texto, eles claramente tiveram sucesso. Para a Anatel chegar à seleção da empresa EAQ foi formado um grupo com representantes da Anatel e das teles. Foram apresentadas quatro propostas de medição: da ABR Telecom (que atualmente cuida da portabilidade numérica), da ISPM, da PWC e do NIC.br, que originalmente estabeleceu os critérios de qualidade.

Ainda de acordo com os mesmo autores, como se trata de uma escolha entre as empresas, a Anatel não soube explicar por que trocar o SIMET, sistema desenvolvido pelo NIC.br, que já vinha sendo utilizado pela própria Anatel. Além disso, a Anatel também descartou a necessidade de acesso ao código-fonte do programa escolhido, por considerar que é um software de mercado, de prateleira, e porque a Anatel não faz desenvolvimento de código.

5.1.2.3 SpeedTeste

O SpeedTeste (SPEEDTESTE, 2017) é um medidor de velocidade de conexão à Internet que está no ar desde 16 de agosto de 2008 como um serviço gratuito. Os servidores onde a ferramenta de medição do SpeedTeste está alocada, ficam nos EUA. O serviço do SpeedTeste tem capacidade para atender até 100 requisições por segundo, sem interferência nos resultados. Os serviços oferecidos pelo SpeedTeste para uso doméstico são: teste gratuito para velocidade de download e taxa de transferência; e

para usuários cadastrados oferece o armazenamento dos testes de velocidade por até um ano. O SpeedTeste oferece também serviços de uso profissional que são cobrados.

5.1.2.4 MinhaConexao

O *site* MinhaConexao (MINHA CONEXAO, 2017) armazena e gera um histórico com os testes dos usuários, informando que podem salvá-lo e imprimi-lo para usar como prova de problemas com sua Internet. Testa as velocidades de *upload* e *download.* Testa a velocidade da Internet Banda larga Fixa e Internet Móvel 3G e 4G. O velocímetro faz o teste de velocidade da Internet de qualquer tipo de provedor: rjnet, Copel, net virtua, velox, speedy, GVT, 3G, 4G, claro, oi, vivo, tim, discada, banda larga, entre outras.

O *site* do MinhaConexão apresenta um *ranking* da velocidade da Internet no Brasil que contém o resultado de mais de 18 milhões de testes feitos, e traz um mapa interativo para encontrar os provedores mais rápidos por região do país. Em resumo, o ranking do MinhaConexão traz: (i) a velocidade dos 10 maiores provedores do país; (ii) a lista das capitais e das cidades mais rápidas; e (iii) a lista dos provedores mais rápidos de cada estado e do Brasil. O software usado no MinhaConexão, em sua forma original, não modificada, é o *phpBB*, produzido, publicado e com direitos reservados ao *phpBBGroup*, que está disponível sob a licença GNU *General Public Licence,* sendo portanto, distribuído gratuitamente.

5.1.2.5 TESTE COPEL

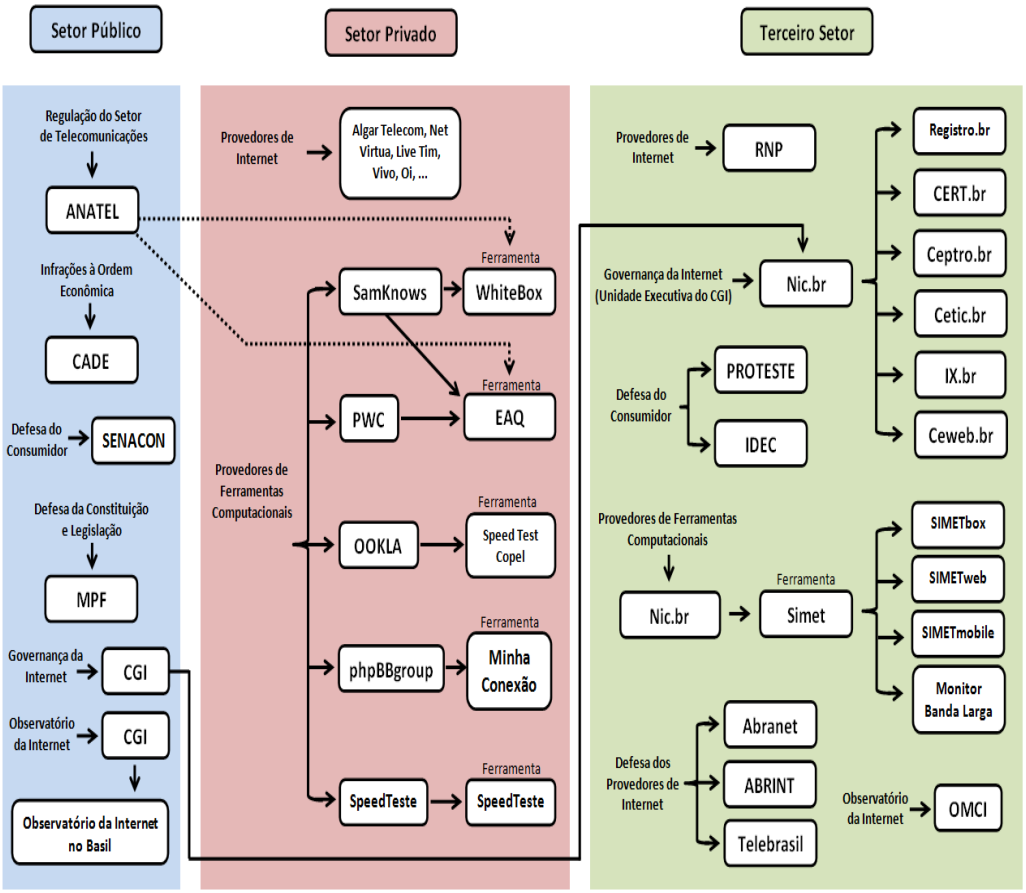
Este não é o *site* oficial da empresa de energia elétrica do estado do Paraná, a Copel. É um *site* onde é ofertado um medidor de velocidade de conexão para usuários da Internet. Este medidor é o Speed Test, da Ookla (TESTE COPEL, 2017) citada nesta tese no item 4.2. O teste é ofertado gratuitamente para que o usuário possa avaliar o serviço de Internet que está recebendo e, com base nos dados apresentados pelo medidor de velocidade, possivelmente questionar o serviço que contratou e demandar melhor desempenho, caso note que o resultado apresentado pelo teste não é compatível com aquilo que foi contratado. O Speed Test Copel oferece a medição da velocidade de

conexão que é fornecida também pelas empresas de Internet Oi Velox, GVT, e Net Virtua, verificando velocidade de *download*, e *upload*, latência, e *jitter*.

5.1.3 Panorama da Internet no Brasil

Para compreender de forma clara o panorama da Internet no Brasil, o relacionamento entre os principais agentes envolvidos com a Internet e, consequentemente, com a Neutralidade da Rede, foi necessário distribuir estes agentes em três setores, de acordo com o seu caráter: setor público, setor privado ou terceiro setor. Os principais agentes levantados e expostos na Figura 10 representam papéis de abrangência nacional. Foram desconsiderados para efeitos desta tese os agentes estaduais e municipais e suas especificidades.

FIGURA 10 - PANORAMA DA INTERNET NO BRASIL



Fonte: O autor (2017).

Importa observar nesta figura as suas principais características, conforme segue.

(i) O setor público é responsável pela regulação, pela manutenção da ordem econômica e pela defesa do prescrito na constituição e na legislação brasileiras, no que concerne ao setor das telecomunicações, onde se insere a Internet. Ao mesmo tempo, o setor público é também responsável pela governança da Internet e pela defesa do consumidor. Observa-se que não há nenhuma ferramenta computacional de monitoramento do tráfego da Internet desenvolvida diretamente pelo setor público.

(ii) O setor privado se responsabiliza pelo provimento da Internet e das ferramentas computacionais que visam medir basicamente a conexão da Internet.

(iii) O terceiro setor, por sua vez, se encarrega de lançar ao mercado da Internet uma mescla de vários agentes que têm por função o provimento da Internet e provimento de ferramentas computacionais, a governança da Internet, a defesa do consumidor e a defesa dos provedores de Internet. Observa-se com isto uma tendência do terceiro setor em exercer um papel híbrido no panorama brasileiro da Internet. Ao mesmo tempo em que o terceiro setor dispõe de agentes que estão representados também no setor público, ele dispõe de agentes que estão representados também no setor privado.

De acordo com a visualização do panorama da Internet no Brasil, é possível inferir que ele lança as bases necessárias à criação do Observatório da Neutralidade da Rede. Isto ocorre na medida em que este panorama mostra de forma clara, a multidisciplinaridade das áreas que o envolve e a necessidade de observação e monitoramento dos agentes envolvidos, quanto ao cumprimento de seus papéis.

5.1.4 Considerações Finais

O debate da Neutralidade da Rede não apenas se insere no contexto da Internet, está vinculado a ela. Conforme já tratado no Capítulo 3 desta tese, há uma lacuna no que se refere à efetividade da aplicação da Neutralidade da Rede no Brasil. Esta lacuna se desnuda ainda mais com a apresentação do panorama nacional, revelando outros aspectos conforme segue.

A lacuna refere-se ao papel da Anatel de regular o setor das telecomunicações e penalizar os ISPs em caso de descumprimento a esta regulação. É notório no Brasil que a Anatel não está atuando de forma efetiva e, tampouco os outros agentes relacionados, como é o caso do CADE e do Senacon. Não se conhece medida efetiva no Brasil,

proveniente destes órgãos, de modo a coibir o comportamento dos ISPs que por vezes ocorre em discordância à normatização da Neutralidade da Rede, como por exemplo, o uso da taxa zero. Outro aspecto desta lacuna é a inexistência de ferramenta computacional, desenvolvida por agentes vinculados ao setor público. E, ainda, que esta ferramenta computacional tenha por função o monitoramento do tráfego da Internet, a fim de detectar diferenciação de tráfego efetuada por algum ISP. E, por fim, que esta detecção possa ser identificada como uma violação à Neutralidade da Rede.

Neste contexto se insere o Observatório da Neutralidade da Rede. Certamente a sua criação não solucionará o debate em torno do tema. Entretanto, este Observatório poderá servir como um instrumento para reunir os vários aspectos que envolvem a Neutralidade da Rede num único ambiente. Este Observatório poderá servir, principalmente, para proporcionar a observação e o monitoramento dos agentes envolvidos com a Internet e a Neutralidade da Rede no Brasil.

5.2 O OBSERVATÓRIO DA NEUTRALIDADE DA REDE (ONR)

Esta seção apresenta a justificativa à criação do ONR. Apresenta também a missão, os valores, o objetivo e as atribuições do ONR. Além disso, mostra a arquitetura do ONR e relata seu lançamento e testes iniciais efetuados por voluntários quanto a sua funcionalidade. Esta funcionalidade refere-se a infraestrutura necessária para monitorar o comportamento dos agentes envolvidos com a Neutralidade da Rede no Brasil a fim de verificar se cumprem seu papel de maneira efetiva e se a legislação pertinente é aplicada.

5.2.1 Justificativa para a criação do ONR

Foi mostrado ao longo desta tese que a gestão razoável do tráfego viabiliza a manutenção da Neutralidade da Rede. Dito de outro modo, a gestão razoável do tráfego cria um ambiente equilibrado, favorável à Neutralidade da Rede. Entretanto, como saber se a gestão da rede efetuada pelos ISPs está sendo feita de forma razoável ou não? Uma resposta é: por meio de ferramentas computacionais que visem monitorar o tráfego a fim de detectar algum tipo de violação à Neutralidade da Rede. Por este motivo, esta

tese levantou e expôs ferramentas existentes. Mas, como saber se estes instrumentos de monitoramento de tráfego estão sendo aplicados pelo órgão regulador, quais são eles, e de que forma estão sendo aplicados? E, ainda, como saber se o órgão regulador está tomando alguma medida cabível, em caso de violação à Neutralidade da Rede, por parte de algum ISP? Uma resposta é: por meio da observação e acompanhamento do comportamento deste órgão regulador e dos demais agentes envolvidos no processo e, também, pelo acompanhamento do assunto pela mídia.

Ao mesmo tempo, é preciso considerar que uma detecção considerada como uma violação à Neutralidade da Rede em um país pode não ser considerada da mesma forma em outro. Por este motivo é necessário monitorar o tráfego da Internet por meio das ferramentas, e acompanhar o desenvolvimento ou avanço da normatização da Neutralidade da Rede, que ocorre nos países, por meio da mídia e dos *sites* dos órgãos governamentais. Por este motivo, esta tese apresentou um panorama mundial da normatização da Neutralidade da Rede no Capítulo 3. No caso do Brasil, a normatização da Neutralidade da Rede ocorreu por meio de Lei e Decreto, conforme relatado neste capítulo. No entanto, é notório que, na prática, não há aplicação da Neutralidade da Rede no país de maneira efetiva, mesmo após a sua normatização.

Conforme exposto anteriormente, a proposta desta tese está justamente neste contexto: a criação de um observatório, como instrumento de monitoramento da Neutralidade da Rede no Brasil, considerando a lacuna existente entre a regulação para a Neutralidade da Rede e a sua efetiva prática. Logo, torna-se imprescindível que sejam estabelecidos os meios basilares para monitorar o que, de fato, decorre em termos da Neutralidade da Rede no Brasil. Para isto foi imperativo levantar e mostrar o panorama atual da Internet no Brasil e o papel dos agentes envolvidos.

Ao longo do tempo de pesquisa e elaboração desta tese não foi localizado no Brasil qualquer observatório da Neutralidade da Rede. Embora existam algumas iniciativas, conforme mostrado no Capítulo 2, nenhuma delas possui a configuração adotada no ONR aqui proposto. O ONR se propõe a reunir e tratar os vários aspectos da Neutralidade da Rede no Brasil, de forma multidisciplinar, conforme imposto pelo debate e aqui exposto.

Também, conforme apresentado até aqui, é possível afirmar que os instrumentos computacionais de monitoramento de tráfego podem detectar violações à Neutralidade da Rede, porém por si sós não equilibram o ecossistema da Internet. A normatização da Neutralidade da Rede por si só, também não garante este equilíbrio. E, da mesma forma,

a criação de um observatório para a Neutralidade da Rede no Brasil, por si só, também não resolve o problema. Todavia, a criação do observatório traz a funcionalidade mínima necessária para o monitoramento do comportamento dos ISPs, da agência reguladora, e dos demais agentes envolvidos no debate da Neutralidade da Rede no Brasil, a fim de obter a dimensão real em termos da efetividade da aplicação da legislação pertinente.

5.2.2 Missão e Valores do ONR

O ONR surge como um dos resultados da pesquisa para elaboração desta tese. Por acreditar que as instituições de ensino e pesquisa guardam entre suas funções o compromisso de devolver à sociedade aquilo que produzem. Ou seja, além de mostrar os resultados de suas pesquisas, estas instituições têm o compromisso de envolver a sociedade, sempre que possível, em suas pesquisas realizadas com recursos públicos. Assim, em cumprimento a este compromisso social, cria-se o ONR.

O ONR surge também em consonância com um dos cinco Grandes Desafios de Pesquisa em Computação no Brasil: o "acesso participativo e universal do cidadão brasileiro ao conhecimento". Estes cinco grandes desafios foram estabelecidos em 2006, em seminário promovido pela SBC (SBC, 2016), com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP).

Do mesmo modo, o ONR é criado como um instrumento de pesquisa, para fins acadêmicos. O ONR está hospedado no Centro de Computação Científica e Software Livre (C3SL) da Universidade Federal do Paraná e seu domínio é observatorio.c3sl.ufpr/neutralidadedarede. O primeiro é um laboratório de pesquisa que tem por princípio ou filosofia de trabalho o desenvolvimento e a disseminação de mecanismos computacionais gratuitos e com código fonte aberto, e a segunda é uma Instituição Federal de Ensino Superior, pública e gratuita. Deste modo, a criação do ONR leva em conta o princípio ou filosofia de trabalho deste laboratório e as características da Instituição onde ele se insere.

E, ainda, igualmente, o ONR não tem qualquer envolvimento político ou fins lucrativos. A gestão do ONR é feita pelo seu Comitê Gestor, que é multidisciplinar, conforme imposto pelo debate da Neutralidade da Rede, e não há restrição de áreas

participantes. Os pesquisadores que atuam no Comitê Gestor do ONR, bem como a participação recebida de usuários individuais ou organizações, de forma eventual ou de forma contínua, são feitas de maneira voluntária.

Em consonância, a Missão do ONR é servir como instrumento de controle social para os vários aspectos que envolvem a Neutralidade da Rede no Brasil. E, identicamente, os Valores que norteiam a atuação do ONR são: Transparência; Compromisso Social; Confiança; Isenção; e Excelência.

5.2.3 Objetivo e Atribuições do ONR

Seguindo a mesma linha de raciocínio, o objetivo do ONR é reunir e fornecer em um único espaço, os meios necessários à observação do comportamento dos agentes envolvidos com a Internet no Brasil, em especial com o debate da Neutralidade da Rede, e à observação do tráfego da rede efetivamente efetuado pelos ISPs. Para atingir ao objetivo a que se propõe, cabe ao ONR cumprir com as seguintes atribuições:

1. Disponibilizar ferramentas de monitoramento de tráfego da Internet que permitam aos usuários de Internet, leigos ou especializados, detectar, porventura, alguma violação à Neutralidade da Rede, de acordo com a regulação brasileira sobre esta matéria.
2. Disponibilizar mecanismo que funcione como um fórum de discussão, um espaço para que os usuários possam relatar os resultados encontrados, por meio do uso das ferramentas de monitoramento de tráfego da Internet, e debater estes resultados com outros usuários, que possam ter vivido a mesma experiência.
3. Reunir e mostrar, em único espaço, os vários aspectos que envolvem o debate da Neutralidade da Rede no Brasil, de modo a permitir a qualquer cidadão que tenha interesse em conhecer o assunto, queira saber qual o efetivo serviço de Internet que recebe ou, ainda, queira acompanhar a atuação dos vários agentes envolvidos, possa fazê-lo.
4. Funcionar como objeto de desenvolvimento de pesquisa para a comunidade acadêmica, e para profissionais das mais diversas áreas, servindo assim como instrumento de auxílio ao desenvolvimento da Internet no Brasil.

5. Servir como base à pesquisa e ao desenvolvimento de novas ferramentas a serem construídas por membros da comunidade técnico e científica de Redes de computadores.

6. Servir como repositório e como difusor de ferramentas ou mecanismos computacionais relacionados ao monitoramento do tráfego da Internet, em especial à Neutralidade da Rede.

7. Servir como um instrumento de pesquisa, fornecendo os subsídios necessários para que a pesquisa na área da Neutralidade da Rede possa ser desenvolvida e os resultados divulgados.

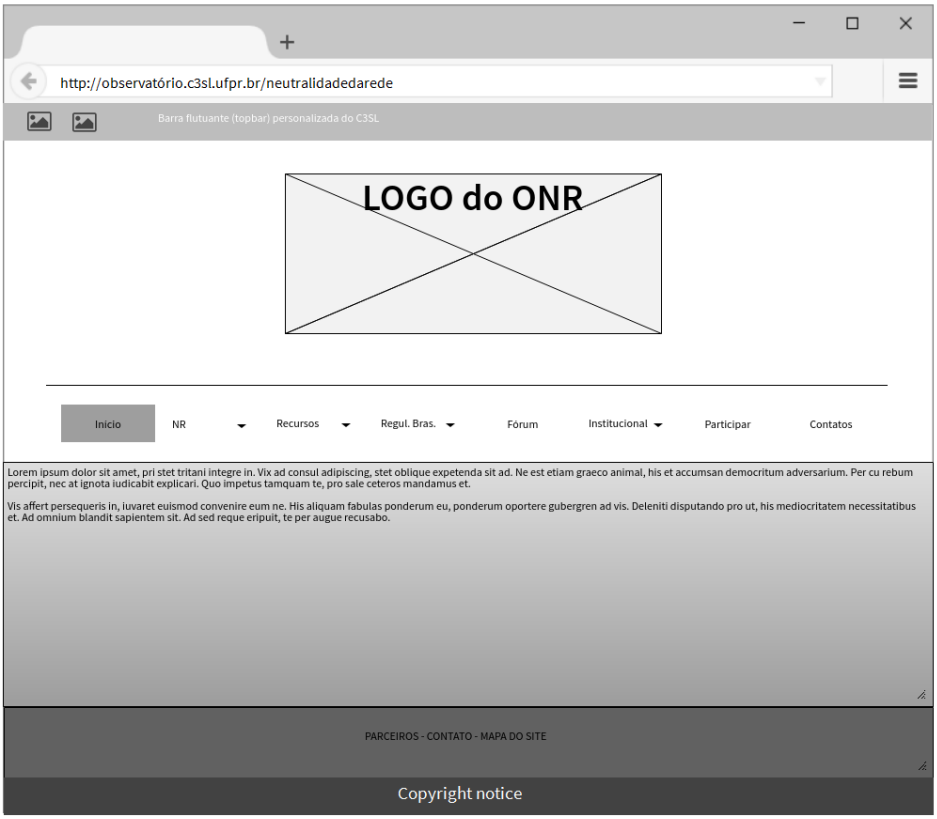
5.2.4 Arquitetura do ONR

Esta subseção mostra de que forma o ONR é construído e os elementos que compõem a sua configuração. Para a tomada de decisão quanto aos elementos que compõem o ONR, foram necessárias algumas discussões com a equipe que atuará como membro do Comitê Gestor do ONR, em especial, os membros responsáveis pela Interação Humano-Computador. Os elementos básicos selecionados para compor o ONR, em sua Versão Inicial para efeitos desta tese, seguem em três formas: *Wireframe*, Mapa do Site e Hierarquia do Menu. São eles: (i) conteúdo sobre a Neutralidade da Rede (o que é, o seu histórico, e os principais aspectos do debate mundial e do debate nacional); (ii) conteúdo sobre a Regulação Brasileira (histórico e legislação); (iii) disponibilização de alguns recursos, tais como as ferramentas de monitoramento do tráfego da Internet, o mapeamento dos IPs e o mapa da Internet; (iv) disponibilização de fórum de discussão e participação dos usuários sobre todos os aspectos que envolvem o debate da Neutralidade da Rede; (iv) conteúdo sobre o ONR (o que é , missão, valores, objetivo, atribuições, e outras informações); (v) conteúdo sobre o Comitê Gestor do ONR (quem são os membros e as suas funções); (vi) convite para participação no ONR (instituições parceiras, desenvolvedores, usuários finais, e outros que possam vir a contribuir com o desenvolvimento do ONR).

5.2.4.1 Wireframe

O *wireframe* do ONR foi projetado após discussões com os membros responsáveis pela Interação Humano-Computador do ONR. Estas discussões tiveram como foco a funcionalidade do ONR e, também, as informações necessárias para formar o conteúdo a ser disponibilizado. A Figura 11 apresenta o *Wireframe* da página inicial do ONR, conforme foi projetado. A Figura 12 expõe de que forma este projeto do *Wireframe*, mostrado na Figura 11, foi executado. A partir do projeto do *Wireframe* foi possível definir e organizar as informações que compõem a página inicial do ONR. Estas informações foram posicionadas de modo a facilitar a sua visualização por parte dos usuários. Dentre estas informações incluem-se: a logomarca desenvolvida para o ONR, o menu principal do ONR e um curto texto de boas-vindas.

FIGURA 11 - *WIREFRAME* PROJETADO PARA O ONR



Fonte: O autor (2017).

FIGURA 12 - *WIREFRAME* EXECUTADO NO ONR

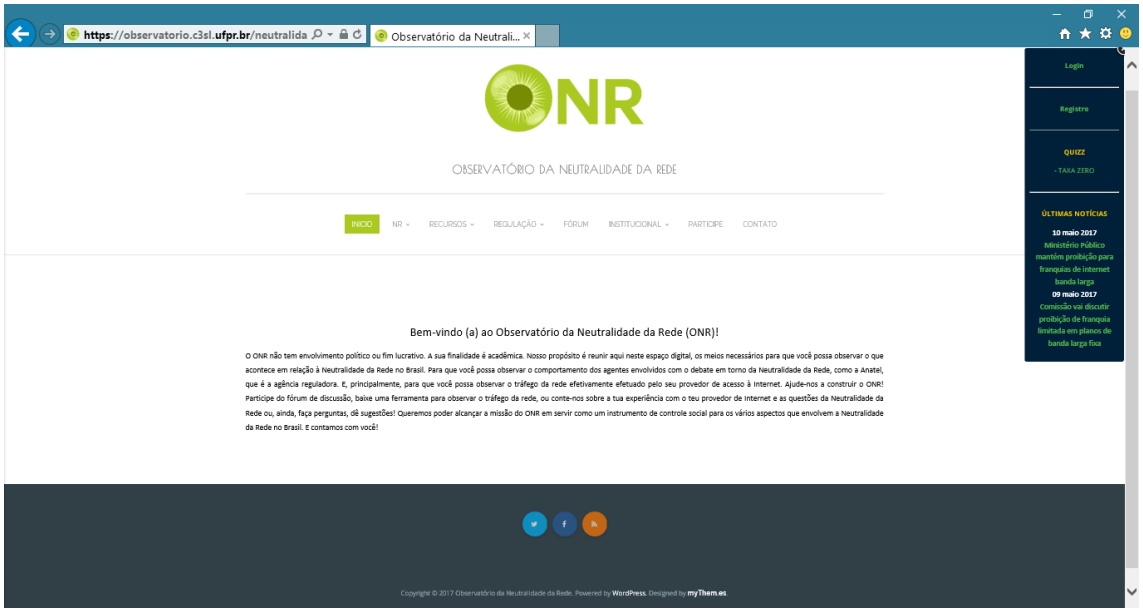
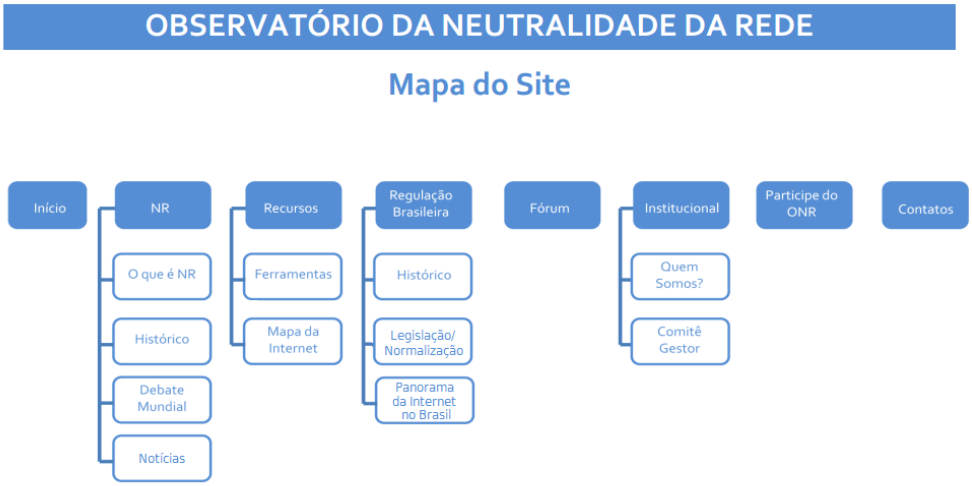


Figura 13 – *Wireframe* Executado no ONR.

5.2.4.2 Mapa do Site

O Mapa do Site do ONR surgiu a partir das discussões e projeto do *Wireframe.* A Figura 13 exibe o Mapa do Site do ONR. Esta figura tem por função fornecer uma visão geral do ONR. Esta figura mostra todo o conteúdo do ONR da forma como foi subdividido, em várias páginas, a partir do menu principal.

FIGURA 13 - MAPA DO SITE DO ONR

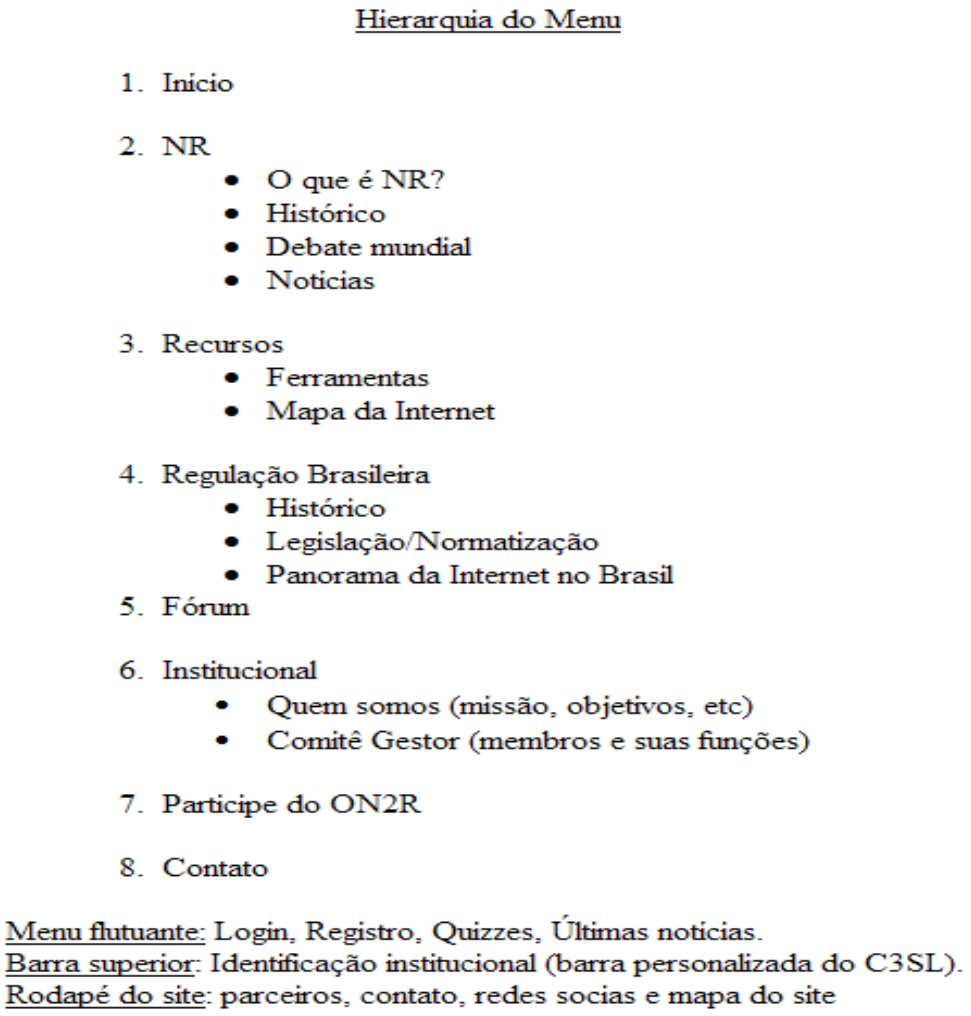


Fonte: O autor (2017).

5.2.4.3 Hierarquia do Menu

A Hierarquia do Menu também surgiu como decorrência das discussões e do projeto do *Wireframe*, efetuados com os membros responsáveis pela Interação Humano-Computador. A Figura 14 apresenta a Hierarquia do Menu do ONR. Esta figura tem por função mostrar a forma como todo o conteúdo foi distribuído e posicionado hierarquicamente no ONR.

FIGURA 14 - HIERARQUIA DO MENU DO ONR



Fonte: O autor (2017).

5.2.5 Considerações Finais

O ONR foi criado como um instrumento de pesquisa para fins acadêmicos e é lançado ao ar em 15 de abril de 2017. Seu lançamento ocorreu com sucesso, já com a

imediata participação e integração de profissionais de várias áreas. Da mesma maneira, observa-se, por meio dos testes iniciais, a participação de usuários finais da Internet no *quizz* da taxa zero, ali disponível, e a participação de usuários especializados, envolvidos com o debate da Neutralidade da Rede, que se voluntariam a fazer parte do ONR de alguma forma. Assim, mesmo que o ONR apresente apenas um curto período de existência, é possível considerar que as bases sobre as quais foi construído são sólidas e fornecem as condições necessárias para que evolua com sucesso a fim de cumprir com a missão à qual se propõe.

CAPÍTULO VI

IMPACTOS DA NORMATIZAÇÃO DA NEUTRALIDADE DA REDE NA EVOLUÇÃO DA INFRAESTRUTURA DA INTERNET: UMA INVESTIGAÇÃO PRELIMINAR DA CORRELAÇÃO

O objetivo deste capítulo é apresentar e relacionar o panorama mundial da evolução da Internet nos últimos anos com o panorama mundial da normatização da Neutralidade da Rede. Esta correlação tem por objetivo investigar se a normatização da Neutralidade da Rede contribui para a ampliação dos investimentos e, consequentemente, contribui para a própria evolução da Internet.

Para obter os dados sobre o número de usuários de Internet em todo o mundo, e a porcentagem da população mundial que estes usuários representam, foi utilizada a base de dados *Internet Live Stats* (INTERNET LIVE STATS, [2017a]). Para obter os dados sobre os investimentos privados em telecomunicações em todo o mundo, foram utilizadas as bases de dados do Banco Mundial (WORLD BANK, 2017a, WORLD BANK, 2017b) e o artigo de Layton e Horney (LAYTON; HORNEY, 2014). Os dados da população mundial também foram obtidos do Banco Mundial. Os dados sobre investimentos públicos em telecomunicações foram obtidos a partir de relatório da Organização para a Cooperação e Desenvolvimento Econômico (*The Organization for Economic Co-operation and Development* (OECD)) (OECD, 2013). Os dados sobre as taxas de adoção acima de 10 Mbps na Internet foram obtidos da Akamai Technologies (AKAMAI, 2017). Finalmente, as notas dos países quanto ao seu índice de Desenvolvimento de TIC (ICT (*Information and Communication Technologies*) *Development Index*), chamada neste trabalho de nota IDI foram obtidas dos relatórios do *United Nations International Telecommunication Union* – ITU, organização responsável pela publicação deste índice (ITU, 2009; ITU, 2010; ITU, 2012; ITU, 2013; ITU, 2014; ITU, 2016). É importante destacar que o Banco Mundial não disponibiliza

dados de investimentos públicos, e que não foram localizados dados de investimentos privados nos relatórios da OECD.

A partir dos dados levantados foram então estabelecidas as seguintes variáveis para os países selecionados, conforme mostradas nas figuras.

(i) Investimento *per capita* em telecomunicações. Esta variável corresponde ao investimento total, público e/ou privado, dividido pelo total da população. Os dados de investimento privado e de população, coletados do *World Bank,* e os dados de investimento público, coletados da OECD, resultaram nesta variável denominada investimento/capita. Os dados de investimento privados *per capita* advindos do trabalho de Layton e Horney, de 2014, foram extraídos e transformados em *per capita* por estes autores a partir dos dados do *Infonetics Research, US Census Bureau e European Commission*. Embora não tenham sido encontrados dados de investimentos públicos e/ou privados para todos os países selecionados em todo o período analisado neste trabalho, optou-se por manter os dados para os anos encontrados, de 1995 a 2014. Esta decisão tomou por base a perspectiva da análise global de tendência dos investimentos, relacionada a outras variáveis. Mesmo que algumas figuras apresentem algumas lacunas, argumenta-se que não representam prejuízo para a análise sobre a evolução aqui proposta.

(ii) Nota do IDI. Esta variável corresponde às notas atribuídas aos países pelo ITU. Os valores das notas deste ranking variam de 1 a 10 e estão disponíveis para os anos de 2002, 2007, 2008, 2010-2013, 2015 e 2016. O IDI (ITU, 2017) está estruturado de forma a atribuir pesos para 3 subgrupos de atributos que, juntos, englobam 11 indicadores. Estes indicadores geram a nota da evolução das Tecnologias de Informação e Comunicação, como segue: (a) infraestrutura e acesso, incluindo assinaturas de telefonia fixa, assinaturas de telefones celulares, largura de banda de Internet internacional (bit/s) por usuário da Internet, percentual de domicílios com computador e percentual de domicílios com acesso à Internet. Este atributo possui peso de 40% sobre a nota; (b) uso, incluindo percentual de indivíduos que utilizam a Internet, assinaturas de banda larga fixa e assinaturas de banda larga móvel. Este atributo também possui peso de 40% sobre a nota; e (c) competências, que se refere à taxa de alfabetização de adultos, taxa de matrículas no ensino médio e taxa de matrículas no ensino superior. Este atributo possui peso de 20% sobre a nota total.

(iii) Taxa de adoção de velocidades acima de 10Mbps. Esta variável corresponde ao percentual da quantidade de conexões que tiveram velocidades superiores a 10 Mbps

entre o 3º trimestre de 2007 e o 4º trimestre de 2016. Os dados de adoção de velocidade extraídos da Akamai foram baseados nos acessos de usuários de todo o mundo, aos aplicativos e conteúdos armazenados em sua rede.

Para construir o panorama mundial da evolução da Internet foram coletados dados disponíveis em várias fontes. Este panorama é formado ao longo do capítulo por um conjunto de gráficos e uma figura. A figura (15) apresenta a porcentagem da população mundial de usuários da Internet. Os Gráficos 1 e 2 mostram, respectivamente, a evolução do investimento público/per capita e a evolução do investimento privado/per capita nos países considerados de renda alta e de renda média alta. O Gráfico 3 apresenta a evolução do investimento privado/per capita nos países considerados de renda alta, de renda média alta e de renda média baixa. Os Gráficos 4 e 5, por sua vez, apresentam, respectivamente, a taxa de crescimento da nota IDI nos países considerados de renda média alta e de renda média baixa, e a taxa de crescimento da nota IDI nos países considerados de renda alta. Os Gráficos 6 e 7 mostram, respectivamente, a evolução da nota IDI nos países considerados de renda média alta e de renda média baixa e a evolução da nota IDI nos países considerados de renda alta. O Gráfico 8 apresenta a média da nota IDI nos Estados-membros da União Europeia. Os Gráficos 9 e 10 apresentam, respectivamente, a taxa da adoção de velocidades acima de 10 Mbps nos países considerados de renda alta e a taxa da adoção de velocidades acima de 10 Mbps nos países considerados de renda média alta e de renda média baixa. E, por fim, O Gráfico 11 mostra a taxa da adoção de velocidades acima de 10 Mbps nos Estados-membros da União Europeia.

Para estabelecer a correlação entre o panorama mundial da evolução da Internet e o panorama mundial da normatização da Neutralidade da Rede, conforme aqui proposto, este capítulo é subdividido em sete seções, como segue. A Seção 6.1 descreve a Neutralidade da Rede como força motriz para o desenvolvimento da Internet. A Seção 6.2 apresenta o panorama mundial da evolução da Internet. A Seção 6.3 mostra a evolução do nível de investimento em telecomunicações. A Seção 6.4 mostra a evolução da nota do IDI. A Seção 6.5 mostra a evolução da taxa de adoção de velocidades acima de 10 Mbps. A Seção 6.6 traz uma discussão sobre o relacionamento entre a Neutralidade da Rede e a evolução da infraestrutura da Internet. Finalmente, a Seção 6.7 apresenta as considerações finais.

6.1. A NEUTRALIDADE DA REDE COMO FORÇA MOTRIZ PARA O DESENVOLVIMENTO DA INTERNET

Conforme apontado no Capítulo 3 desta tese, para que a Neutralidade da Rede seja efetivamente aplicada, é necessário estabelecer normatizações ou regulações, na forma de regras, leis, diretrizes, entre outros, a serem seguidas pelos ISP's. Sem normatização, os ISPs têm autonomia para decidir como devem efetuar o gerenciamento de tráfego nas suas redes. Porém, estas decisões tomadas pelos ISPs podem acarretar em prejuízo aos usuários e serem nocivas para a evolução da Internet, conforme ela foi concebida. Deste modo, é por meio da normatização que as regras para gerenciamento de tráfego razoável são estabelecidas e, a partir dela, é que os agentes de controle dos governos, responsáveis pelo setor de Telecomunicações, podem tomar providências cabíveis, a fim de monitorar, punir ou coibir práticas perniciosas a este setor econômico.

No contexto econômico, a discussão que permeia a normatização da Neutralidade da Rede envolve questões como a manutenção da competitividade e da inovação na Internet, em consonância com a evolução da rede, que, nesta tese, é definida como a manutenção ou incremento dos investimentos visando à ampliação e modernização da infraestrutura da rede. Esta evolução deve ocorrer de modo a permitir que a Internet venha a suportar o crescimento contínuo de usuários, bem como de serviços e produtos disponíveis na rede.

Para alguns autores, a Neutralidade da Rede é um esforço para criar regulações que definam quais práticas de gerenciamento de tráfego da rede são permitidas ou proibidas, considerando a concorrência, a competição, a inovação, o gerenciamento da rede neutro sem distinção de preço, tendo em vista os dados trafegados, bem como sua origem e seu destino (LEMLEY; LESSIG, 2001; WU, 2002; VAN SCHEWICK, 2010; ECONOMIDES; TAG, 2012).

Além disso, a Internet deve ser mantida como uma estrutura universal e livre para todos, sendo que o gerenciamento de seu tráfego deve ser guiado por motivos técnicos e éticos, e não políticos ou comerciais (CGI, 2009b; UN, 2012). Desta forma, as regulações da Neutralidade da Rede devem seguir os preceitos da não discriminação na rede e da universalização do acesso, possibilitando aos usuários a liberdade de escolha e o controle sobre suas atividades na rede. Além disso, as regulações da Neutralidade da Rede devem imputar aos ISPs a transparência das informações sobre a

qualidade do serviço que prestam e as políticas adotadas para o gerenciamento do tráfego em suas redes (INTERNET SOCIETY, 2015b).

Em contraponto, alguns autores afirmam que em uma indústria de rápida evolução, a adoção da Neutralidade da Rede é prejudicial para a Internet, pois priva os ISPs de encontrar alternativas de serviços, produtos ou até mesmo modelos de negócio que ofereçam melhor custo-benefício (YOO, 2005; HAHN; WALLSTEN, 2006; THE STATE…, [2014]). Por este motivo, estes autores acreditam que os governos deveriam focar na remoção das barreiras regulatórias que, de acordo com os mesmos autores, dificultam a evolução da Internet. Assim, os governos deveriam dar liberdade aos ISPs para adotarem as práticas de gerenciamento de tráfego que considerarem adequadas, inclusive permitindo acordos comerciais com os provedores de conteúdo. Por trás desta linha de raciocínio está a consideração de que não é responsabilidade apenas dos ISP's garantir a evolução da infraestrutura da Internet, mas de todos os atores envolvidos com a rede.

Por outro lado, autores e entidades como a OECD (*Organization for Economic Co-operation and Development*) afirmam que as discussões sobre a Neutralidade da Rede são essenciais para garantir e incentivar a inovação, a concorrência e o investimento na Internet (OECD, 2016; VAN SCHEWICK, 2010). De acordo com esta linha de pensamento, o debate da Neutralidade da Rede entra em processo de regulação naturalmente, conforme amadurece nos países. A discussão em torno dos pontos cruciais a fim de manter a evolução da Internet faz parte deste processo. Esta evolução deve ocorrer de modo que os investimentos na infraestrutura da rede possam suportar o crescimento contínuo do número de usuários, bem como a ampliação contínua na oferta de conteúdo e serviços disponibilizados na rede. Neste sentido, a (FCC, 2010) ressalta que uma Internet neutra fomenta um círculo virtuoso de inovação no qual novos usos da rede, incluindo novos conteúdos, aplicações, serviços e dispositivos, criam uma maior demanda de usuários finais de banda larga, o que impulsiona a evolução da própria infraestrutura da rede, levando a novas formas de uso inovadoras.

Este círculo virtuoso ocorre da seguinte forma: (i) as melhorias ou as ofertas de baixo custo introduzidas pelos provedores de conteúdo, aplicativos, serviços e dispositivos, estimulam a demanda dos usuários finais e incentivam os ISPs a expandir suas redes e a investir em novas tecnologias de Internet; (ii) os desenvolvedores criam conteúdos e aplicativos que os consumidores desejam, o que os leva a contratarem, dos ISPs, os serviços e equipamentos. Isto, por sua vez, impulsiona o investimento na

infraestrutura da rede e em novas tecnologias em resposta à demanda do consumidor; (iii) essas melhorias na rede geram novas oportunidades para os ISPs, estimulando-os a inovar ainda mais; (iv) cada rodada de inovação aumenta o valor da Internet para os ISPs, as empresas on-line e os consumidores. No entanto, a FCC (FCC, 2010) ressalta também que a continuação deste círculo virtuoso depende de baixas barreiras à inovação e à entrada dos ISPs, que impulsionam a demanda dos usuários finais. Restringir a capacidade dos ISPs de alcançar os usuários finais e limitar a capacidade dos usuários finais de escolher os ISPs reduz a taxa de inovação na borda da rede e, provavelmente, a taxa de melhorias na infraestrutura da rede (FCC, 2010).

A União Europeia, por intermédio do BEREC, em 2016, ressalta que pretende proteger os usuários finais e, simultaneamente, garantir o funcionamento contínuo do ecossistema da Internet como um motor de inovação (BEREC, 2016b). A União Europeia considera que a Internet desenvolveu-se ao longo das últimas décadas como uma plataforma aberta para inovação, com baixas barreiras de acesso para usuários finais, para provedores de conteúdo, aplicativos e serviços, e para os ISPs. O Japão, por sua vez, por meio de seu agente regulador, o MIAC, enfatiza em seu relatório do painel sobre a Neutralidade da Rede, de 2008, que realizou suas próprias investigações sobre um arcabouço para manter a Neutralidade da Rede. Em tal contexto, o Japão julgou que se tornou necessário investigar o arcabouço para suportar o ônus do custo do fortalecimento das redes de comunicação, que permita um aumento acentuado do tráfego. O arcabouço de um esforço conjunto dos interessados, incluindo os provedores de conteúdo, os ISPs, as operadoras de telecomunicações e os usuários (MIAC, 2008).

A Coréia do Sul, visando obter uma taxa de crescimento econômico anual superior a 4% em 2013, por meio da KCC, seu órgão regulador do setor de Telecomunicações, estabelece que precisará fazer novos investimentos em novas redes, para atender a demanda de tráfego cada vez maior (KCC, 2012). O Canadá, por meio da CRTC, enfatiza que o investimento na rede é uma ferramenta fundamental para lidar com o congestionamento e deve continuar a ser mantido pelos ISPs (CRTC, 2009). O Chile, por sua vez, em sua Lei 20.453 de 2010 que trata da Neutralidade da Rede, determina que os ISPs publiquem em seu site a velocidade ofertada e a qualidade dos enlaces de comunicação, diferenciando entre as conexões nacionais e internacionais, assim como a natureza e garantias do serviço e outras informações relativas às características do acesso à Internet ofertado (CHILE, 2010), incentivando desta forma, o investimento contínuo na infraestrutura da rede, por parte dos ISPs.

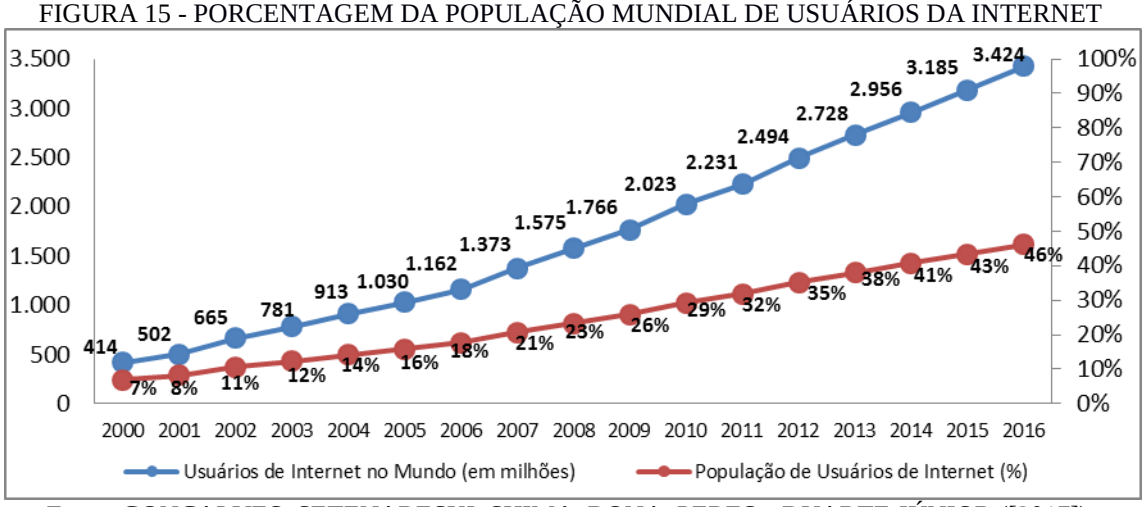
6.2. PANORAMA MUNDIAL DA EVOLUÇÃO DA INTERNET

Na medida em que o número de seus usuários se aproxima dos 4 bilhões (INTERNET WORLD STATS, 2017), não resta dúvida quanto à importância da Internet. A Internet tornou-se primordial no apoio à inovação, ao crescimento econômico e ao progresso sociocultural da sociedade. Desde suas origens nos anos 1960 como um projeto das forças armadas americanas, mais especificamente do DARPA (*Defense Advanced Research Projects Agency*), passando pela incorporação dos protocolos TCP/IP (*Transmission Control Protocol/Internet Protocol*) nos anos 1980 até os dias atuais, a Internet cresceu exponencialmente e diversas questões sobre sua arquitetura, funcionamento, gerenciamento e uso têm chegado à luz da discussão.

Neste cenário, uma vez que cresce o número de usuários, aumentam suas demandas por mais capacidade de rede, na mesma proporção em que mais serviços e produtos são disponibilizados, e a própria tecnologia na Internet evolui. O resultado é que há um impacto do lado dos ISP's, que precisam acompanhar as demandas, ampliando e modernizando suas infraestruturas. Neste contexto, destaca-se que o aumento contínuo de demanda, seguido por atualização da infraestrutura de rede, leva a congestionamentos ocasionais inevitáveis. Esta é uma das razões pelas quais é permitido aos ISP's o uso de técnicas de gerenciamento de tráfego: para desobstruir a passagem dos dados na rede e manter a qualidade dos serviços ofertados.

A necessidade de conexões de grande largura de banda tem aumentado continuamente nas últimas décadas na Internet. Atualmente, existem mais de 1 bilhão e 200 milhões de *websites* que oferecem conteúdo e serviços na Internet (INTERNET LIVE STATS, [2017b]). A Figura 15 apresenta a evolução global do número de usuários de Internet em todo o mundo, bem como uma curva com a porcentagem da população mundial que estes usuários representam. Como pode ser observado nesta figura, o crescimento tem sido contínuo e a taxa de crescimento é aproximadamente linear.

FIGURA 15 - PORCENTAGEM DA POPULAÇÃO MUNDIAL DE USUÁRIOS DA INTERNET



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

A ITU e a UNESCO (ITU; UNESCO, 2016) consideram a evolução da Internet no mundo não apenas em termos do aumento das velocidades das conexões disponíveis, mas também em termos de sua cobertura, por exemplo, considerando áreas rurais e urbanas e a própria universalização do acesso à rede.

Em seu relatório de 2016, a OECD considera que as discussões sobre a Neutralidade da Rede são essenciais para garantir e incentivar a inovação, a concorrência e o investimento na Internet. A OECD considera ainda que a discriminação de tráfego por meio de bloqueio e filtragem é prejudicial, pois afeta a disponibilidade dos serviços e de conteúdo. Neste contexto, a Neutralidade da Rede é colocada como o princípio que garante o funcionamento correto da rede, mesmo com o aumento da demanda, tanto em número de usuários quanto na quantidade de serviços e conteúdos disponíveis (OECD, 2016).

É preciso garantir a evolução da rede, de forma que os conteúdos e serviços sejam acessados pelos usuários com a qualidade necessária. A evolução da rede pode ser vista sob diversos aspectos. Por exemplo, governos regulam a entrada de novos ISP’s e incentivam o desenvolvimento da infraestrutura da rede para a manutenção da qualidade do serviço de acesso à Internet. Tendo em vista as crescentes demandas, existe a necessidade contínua de investimentos na construção e ampliação de infraestrutura da rede, inclusive para viabilizar o serviço de acesso à Internet para áreas remotas e/ou rurais e um número cada vez maior de cidadãos, independente de sua condição econômica. É fácil constatar, entretanto, que cada país estrutura suas diretrizes de maneira muito própria, considerando questões geográficas, populacionais, PIB, concorrenciais, entre outras.

Para compreender o papel dos governos na evolução da Internet, é particularmente relevante o trabalho de Silva e Biondi (2012). Segundo estes autores, após a crise econômica mundial de 2008, diversos governos intensificaram as ações para incentivar a evolução e o acesso universal à Internet, embora existissem várias iniciativas anteriores. Estes governos entenderam que medidas direcionadas à universalização da Internet tinham potencial concreto para auxiliar na retomada dos níveis de crescimento das atividades econômicas. Algumas destas iniciativas governamentais, apresentadas por Silva e Biondi (2012) consideram que, de modo geral, a universalização do acesso à Internet caracteriza-se pela participação governamental na estruturação de infraestrutura de redes nacionais. Exemplos destas iniciativas, anteriores e posteriores à crise de 2008 incluem (em ordem alfabética): a Austrália, que instituiu em 2004 o plano *Australia's National Broadband Strategy*; o Brasil, que iniciou o Programa Nacional de Banda Larga em 2010; o Canadá, que instituiu em 2009 o *Canada's Economic Action Plan* e o *Broadband Canada: Connecting Rural Canadian*; dos Estados-membros na União Europeia, a Finlândia, que instituiu o *National Plan of Action for Improving the Infrastructure of the Information Society* em 2008; O Reino Unido, que iniciou o Plano Nacional *Digital Britain*, em 2009; e a França, que iniciou o *France Numérique* 2008-2010 e o *France Numérique* 2012-2020, em 2011; o Japão, que iniciou em 2006 o plano estratégico *U-Japan* e em 2010 o *New Broadband Super Highway*; os Estados Unidos, que instituiram o *National Broadband Plan* em 2010; a África do Sul, que iniciou a *Policy Broadband for South Africa* em 2010; e Coréia do Sul, que implantou a primeira estratégia em 2004, a IT 839, com uma atualização em 2006; e em 2011 iniciou o *GIGA Korea Project.*

As iniciativas variam de país para país, pois envolvem questões como o tamanho da população, o rendimento médio dos cidadãos, a extensão do território geográfico do país, as infraestruturas de telefonia já instaladas e disponíveis para uso, e o entendimento sobre o princípio da Neutralidade da Rede, entre outros. É possível destacar as diferenças relativas ao tamanho do território geográfico, que é um fator que afeta o aumento da infraestrutura da rede. O Japão e a Coréia do Sul, por exemplo, possuem territórios menores. O fator linguístico, que se relaciona com as iniciativas de capacitação dos usuários no manuseio da tecnologia é uma dificuldade encontrada na África do Sul. Além disso, o poder econômico dos cidadãos dos países interfere diretamente na contratação dos planos de conexões, ofertados pelos ISPs, visto que o

aumento dos usuários é o que justifica a necessidade do incremento da infraestrutura da rede.

Neste sentido, manter a evolução da infraestrutura da rede é um desafio real e necessário a ser enfrentado pelos governos. Observa-se que o principal vetor para suportar o crescimento contínuo da Internet é a manutenção dos investimentos em sua infraestrutura. A melhoria e o aumento na infraestrutura da rede fornecem as condições necessárias para a manutenção dos princípios da Neutralidade da Rede, sem que haja necessidade de discriminação de tráfego por parte dos ISPs. Embora, isso signifique que quanto melhor a infraestrutura da rede menor seja a possibilidade de violação dos princípios da Neutralidade da Rede, vale destacar que acordos comerciais entre os ISPs, e entre os ISPs e os provedores de conteúdo, são passíveis de serem praticados, mesmo com a existência de infraestrutura de rede adequada ao crescimento na adesão dos usuários.

6.3. EVOLUÇÃO DO NÍVEL DE INVESTIMENTO EM TELECOMUNICAÇÕES

O objetivo desta seção é analisar a evolução do nível de investimento em telecomunicações de diversos países, por meio dos dados extraídos da base de dados do Banco Mundial[7]. O Banco Mundial classifica os países em níveis, de acordo como a sua renda, como segue: Renda Alta (*High Income*); Renda Média e Baixa (*Low & Middle Income*); Renda Baixa (Low Income); Renda Média Baixa (*Lower Middle Income*); Renda Média (*Middle Income*); Renda Média Alta (*Upper Middle Income*).

Para efeitos desta tese foram selecionados os seguintes países, classificados como Renda Alta (RA): Austrália, Canadá, Chile, Japão, Nova Zelândia, Noruega, Coréia do Sul, Estados Unidos e União Europeia (a maioria dos seus Estados-membros entra nesta classificação). Foram selecionados também os seguintes países classificados como Renda Média Alta (RMA): Brasil, Colômbia, China, México, Rússia e África do Sul. E, foi selecionada ainda a Índia, como único país da classificação Renda Média Baixa (RMB). Estes países compuseram no Capítulo 3, o panorama mundial da normatização da Neutralidade da Rede. Aparecem novamente aqui para que se possa

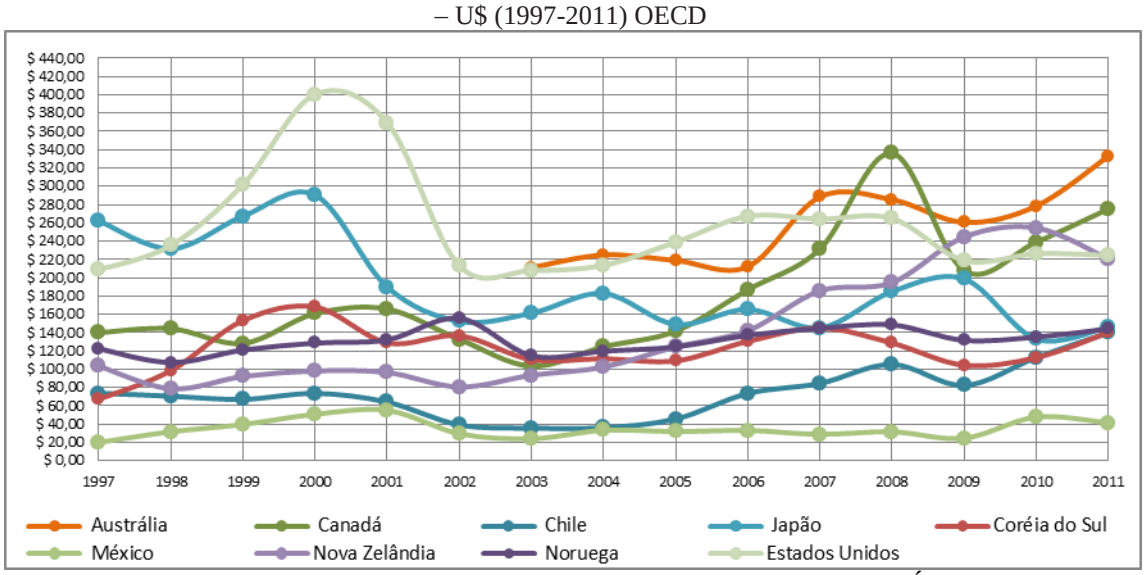
[7] data.worldbank.org

formar com eles o panorama da evolução da Internet e investigar a correlação com a Neutralidade da Rede.

É possível afirmar que o volume de investimento é um dos dados mais importantes para compreender a evolução, no sentido de crescimento, da infraestrutura de telecomunicações nos diversos países. Para isso, considerou-se a relação do investimento per capita em diversos países, levando em conta tanto o investimento público, quanto o investimento privado.

O Gráfico 1 apresenta os investimentos público/per capita nos Países RA e no México, classificado como país RMA. Isto porque o México foi o único país RMA com dados de investimento público na base de dados da OECD. Este Gráfico mostra que os Estados Unidos são o país que apresenta o maior investimento público/per capita. Isto ocorre no ano 2000. O segundo maior investimento público/per capita é apresentado pelo Canadá, no ano de 2008, seguido pela Austrália em 2011. Na sequência aparece o Japão, também em 2000, mesmo ano dos Estados Unidos. A Nova Zelândia, por sua vez, mostra crescimento contínuo em seu investimento público/per capita, de 2003 a 2011, quando sofre uma queda. A Noruega mostra dois momentos de maior volume de investimento público/per capita, sendo o primeiro em 2002 e o segundo em 2008. Neste Gráfico é possível verificar ainda que o Chile e o México, ambos países da América Latina, sendo respectivamente o primeiro classificado como RA e o segundo como RMA, são os dois países que exibem os menores volumes de investimento público/per capita em todo o período.

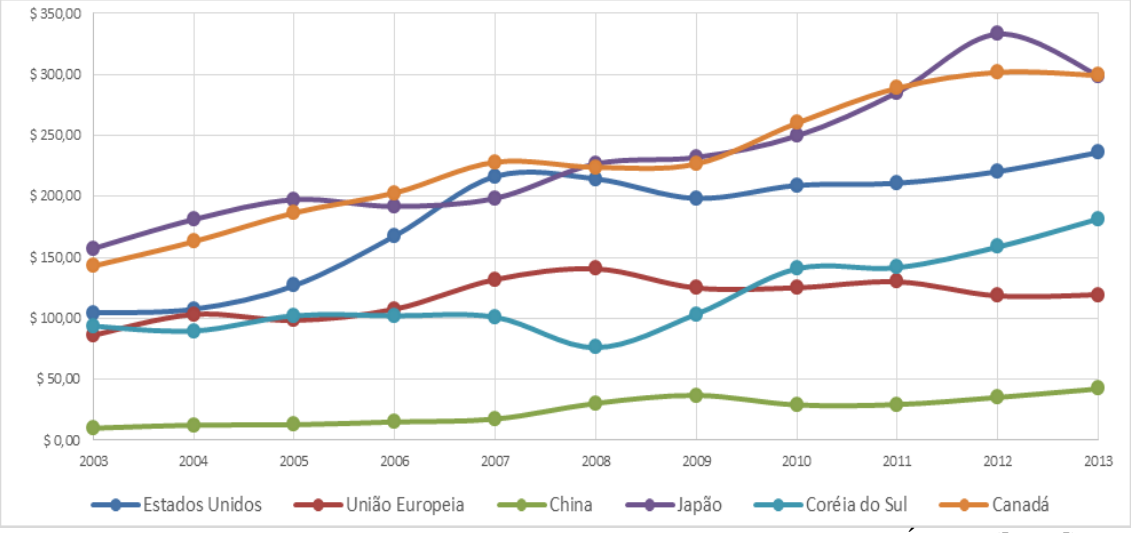
GRÁFICO 1 - EVOLUÇÃO DO INVESTIMENTO PÚBLICO/PER CAPITA NOS PAÍSES RA E RMA – U$ (1997-2011) OECD



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

No Gráfico 2 são apresentados os dados de investimento privado/per capita dos países RA: Estados Unidos, Japão, Coréia do Sul, Canadá e União Europeia, cuja maioria dos Estados-membros pode ser classificada nesta categoria; e os dados de investimento privado/per capita da China, considerada país RMA. Isto porque a China foi o único país RMA com dados de investimento privado encontrados no artigo de Layton e Horney. A partir da observação dos Gráficos 1 e 2 em conjunto, é possível observar, por exemplo, que os Estados Unidos mantêm crescimento mais constante no investimento privado que no público. É possível observar também que o Japão mostra algumas oscilações no investimento público no período, apresentando picos em 2000 e 2009. No entanto, no investimento privado, o Japão mantém crescimento constante a partir de 2006, com seu pico em 2012. A Coréia do Sul mostra um comportamento similar ao do Japão, com crescimento contínuo no investimento privado a partir de 2009, e seu pico em 2013, enquanto o Canadá mostra um pico no investimento público em 2008, e no investimento privado em 2012, mesmo ano do Japão. O Gráfico 2 mostra também a evolução do investimento privado/per capita da União Europeia e da China. Ambas apresentam poucas oscilações, tendo a União Europeia alcançado seu pico em 2008 e a China em 2013.

GRÁFICO 2 - EVOLUÇÃO DO INVESTIMENTO PRIVADO/PER CAPITA NOS PAÍSES RA E RMA (LAYTON; HORNEY, 2014) – U$ (2003-2013)

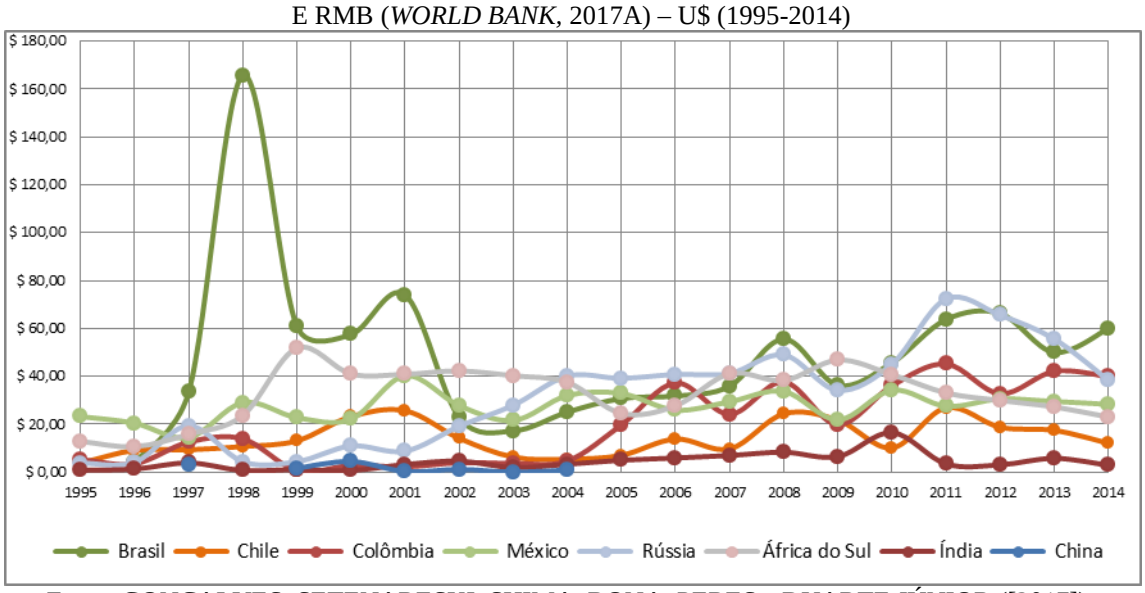


Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

O Gráfico 3 mostra o investimento privado/per capita dos países RA, RMA e RMB, conforme estavam disponíveis na base de dados do Banco Mundial. O Gráfico 3 mostra que o Brasil, país RMA, alcançou as maiores oscilações e também os maiores picos de investimento privado, em relação a todos os demais países apresentados, sendo

seguido, respectivamente, pela Rússia e pela África do Sul, também países RMA. Por outro lado, os países que mostram o menor número de oscilações e também os menores volumes de investimento privado/per capita são, respectivamente, a China, país RMA, e a Índia, país RMB. A Colômbia, por sua vez, embora também esteja entre os menores volumes de investimento privado/per capita até 2004, a partir daí, mesmo apresentando algumas oscilações de queda, aumentou em muito o seu volume de investimento privado/per capita no restante do período analisado. Já o México, país RMA, aparece em uma posição intermediária e o Chile, país RA, mostra um volume de investimento privado/per capita inferior ao da maioria dos países RMA apresentados.

GRÁFICO 3 - EVOLUÇÃO DO INVESTIMENTO PRIVADO/PER CAPITA NOS PAÍSES RA, RMA E RMB (*WORLD BANK*, 2017A) – U$ (1995-2014)



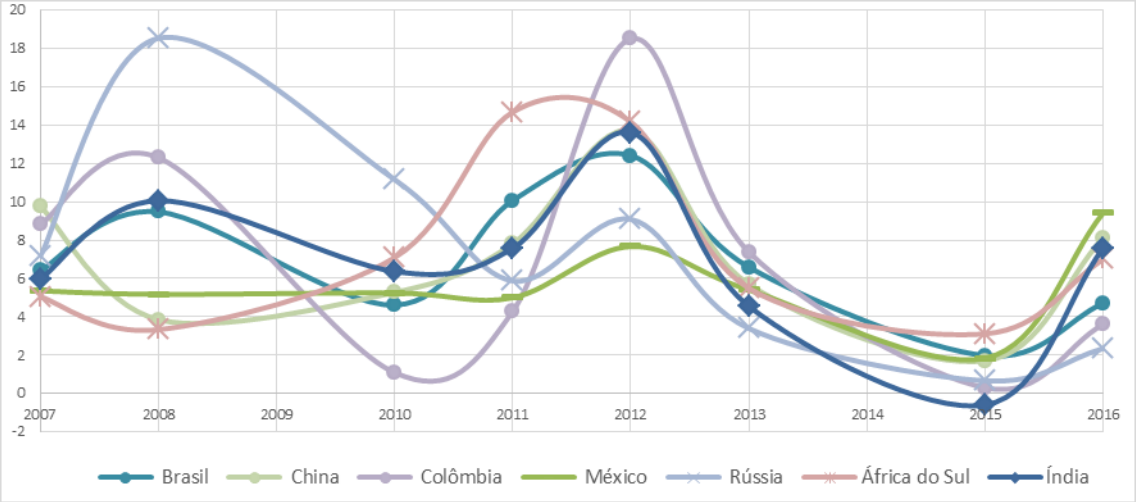
Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

6.4. EVOLUÇÃO DO ÍNDICE DE DESENVOLVIMENTO DE TIC (IDI)

Outro indicador importante da evolução das telecomunicações é a nota IDI. Dos Gráficos 4 a 8 podem ser observados, no eixo vertical, a taxa de crescimento, ou a evolução das notas IDI dos países e, no eixo horizontal, os anos em que foram encontrados os dados. Ao analisar os Gráficos 4 e 5 em conjunto, observa-se que a Rússia e a Colômbia se destacam por atingir a maior taxa de crescimento das notas IDI, tanto em relação aos outros países do Gráfico 4, classificados como RMA e RMB, quanto em relação aos países RA, apresentados no Gráfico 5. O Brasil, a África do Sul e a Índia também ultrapassam as taxas de crescimento das notas IDI dos países RA.

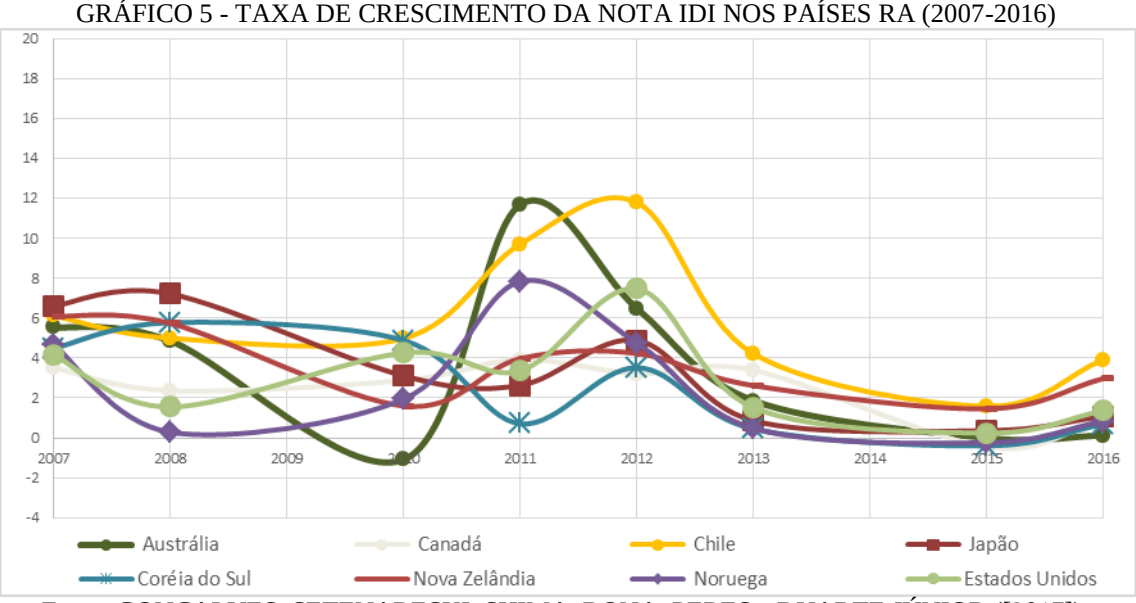
O Gráfico 5 mostra que os Países RA tem um comportamento muito semelhante entre si, alcançando o pico na taxa de crescimento da nota IDI em 2011 e 2012 e, após este período, apresentando queda na taxa de crescimento. Nos Gráficos 4 e 5 pode-se destacar que o Chile, classificado como RA, teve pico de crescimento no mesmo ano em que o Brasil, classificado como RMA, e com uma taxa bem próxima à dele.

GRÁFICO 4 - TAXA DE CRESCIMENTO DA NOTA IDI NOS PAÍSES RMA E RMB (2007-2016)



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

GRÁFICO 5 - TAXA DE CRESCIMENTO DA NOTA IDI NOS PAÍSES RA (2007-2016)

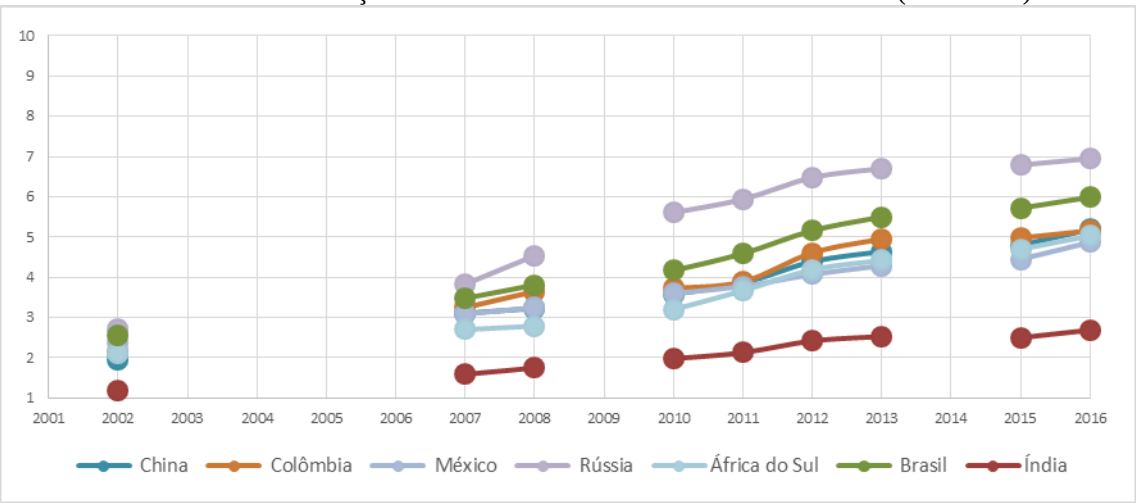


Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

Ao analisar os Gráficos 6 e 7 é possível inferir que as notas IDI para os países RMA e RA evoluem no mesmo ritmo, mas os países RMA mantêm suas notas IDI mais baixas que dos países RA. Portanto, é necessário aumentar os investimentos nos países RMA para que atinjam um ponto de convergência. Caso contrário, os países RMA

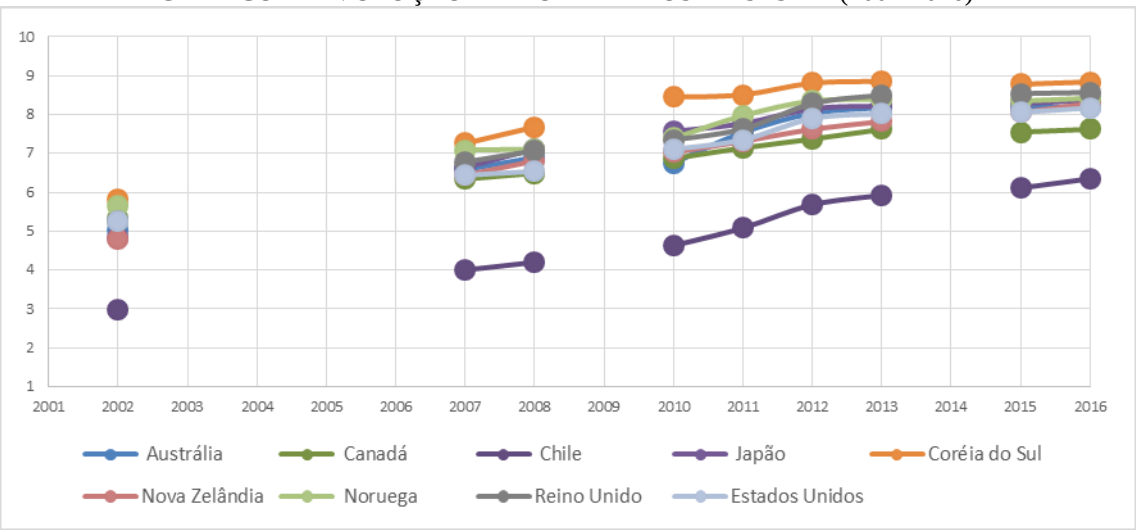
sempre ficarão para trás e sofrerão as consequências permanentes relacionadas à sua posição inferior.

GRÁFICO 6 - EVOLUÇÃO DA NOTA IDI NOS PAÍSES RMA E RMB (2002-2016)



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

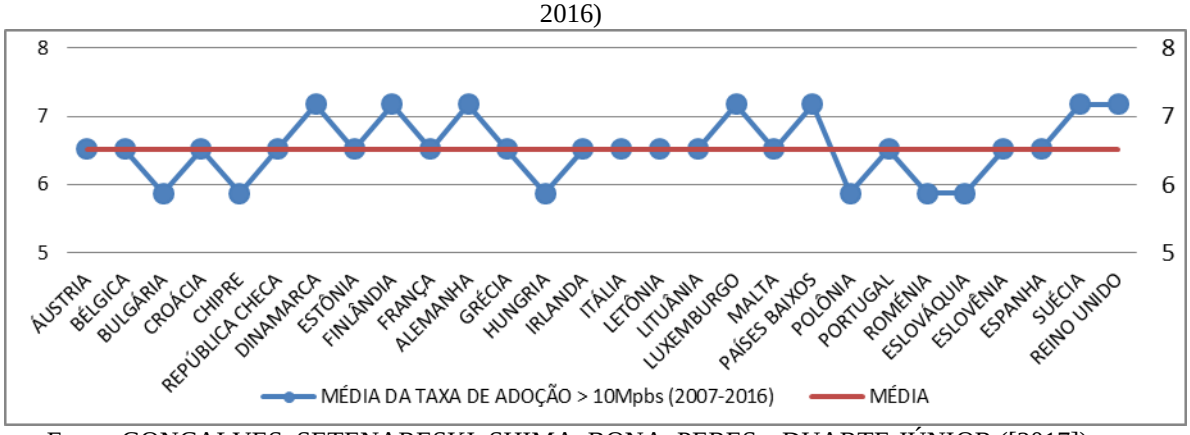
GRÁFICO 7 - EVOLUÇÃO DA NOTA IDI NOS PAÍSES RA (2002-2016)



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

O Gráfico 8 apresenta a média da nota IDI dos Estados-membros da União Europeia. Para elaborar este gráfico, primeiro foi necessário verificar a média da nota IDI para todos os Estados-membros e também para cada ano para o qual foram obtidos dados. A partir do resultado encontrado, foi calculada uma média única para todo o período analisado e para todos os Estados-membros. A média encontrada foi 6,52. Após isto, foi necessário estabelecer a faixa da média para a nota do IDI para todos os Estados-membros. Ou seja, os Estados-membros foram classificados como acima da média, quando sua média da nota IDI ficou entre 6,52 e 7,17; e classificados como abaixo da média, quando sua média da nota IDI ficou entre 5,87 e 6,52.

GRÁFICO 8 - MÉDIA DA NOTA IDI NOS ESTADOS-MEMBROS DA UNIÃO EUROPEIA (2007-2016)



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

Em síntese, a análise conjunta de todos os gráficos apresentados até aqui, mostra que os países RA possuem as notas IDI mais altas e, consequentemente, possuem volume de investimento/per capita maior que o investimento/per capita dos países RMA, à exceção do Chile. Entretanto, é possível sugerir que há uma tendência de aproximação dos países RMA, como por exemplo, o Brasil e a Rússia. Mesmo assim, a aparente maior inclinação da curva de evolução da nota IDI dos países RMA, mostra que as notas alcançadas ao longo de todo o período indicam que dificilmente eles alcançarão os países RA. Isto porque os países RMA evoluem num mesmo ritmo dos países RA, o que significa que há uma tendência a manterem a lacuna entre os dois grupos de países. Desta forma, os países RMA precisariam ter um volume de investimento/per capita muito mais alto, de forma a aumentar suas notas IDI muito mais rapidamente que as notas IDI dos países RA.

6.5. EVOLUÇÃO DA TAXA DE ADOÇÃO DE VELOCIDADES ACIMA DE 10 MBPS

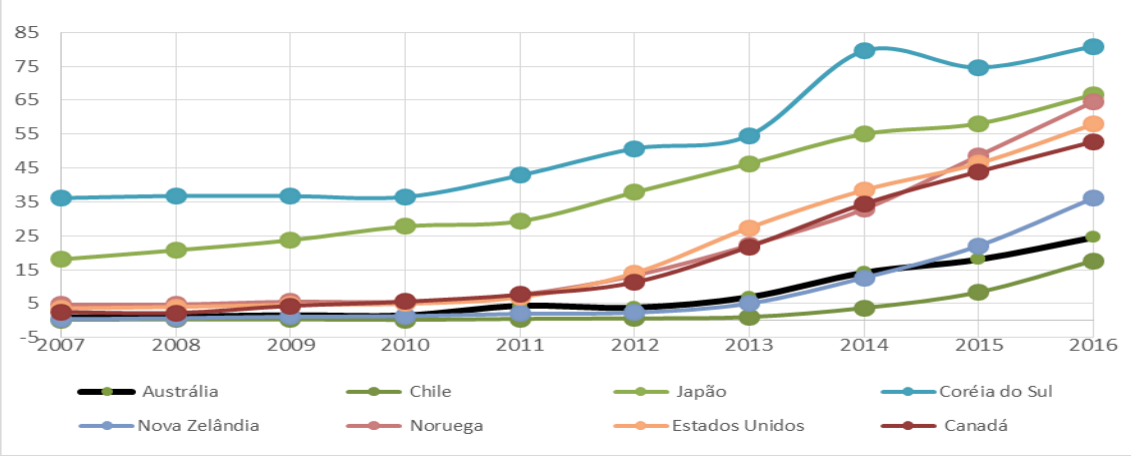
Outro indicador importante da evolução da Internet é a taxa de adoção de velocidades acima de 10 Mbps. Quanto maior a taxa de adoção de velocidades neste patamar em um determinado país, mais o uso da Internet pode ser considerado universalizado e, também, é possível concluir que existe uma ampla infraestrutura instalada. Para efeitos desta tese, considera-se que velocidades acima de 10 Mbps são razoáveis para usuários acessarem conteúdos considerados mais pesados, como por exemplo, jogos ou vídeos online.

Na medida em que a infraestrutura da rede expande, maiores velocidades de acesso são disponibilizadas, juntamente com conteúdos ainda mais pesados.

No Gráfico 9, é possível verificar os percentuais relativos à quantidade de conexões com velocidades superiores a 10 Mbps, nos países RA. Em linhas gerais, o Gráfico mostra que todos os países RA tiveram crescimento contínuo, e que, neste crescimento houve destaque para a Coréia do Sul. De forma específica, observa-se no Gráfico 9, que os maiores percentuais correspondem, respectivamente, à Coréia do Sul com 80,88% e o Japão, com 66,62%. A seguir encontram-se a Noruega, com 64,54%, os Estados Unidos, com 57,93%, e o Canadá, com 52,78%. O Gráfico 9, mostra também que os menores percentuais relativos à quantidade de conexões que tiveram velocidades superiores a 10 Mbps encontram-se, respectivamente, no Chile, com 17,65%, e na Austrália, com 24,5%. A Nova Zelândia vem a seguir, numa posição intermediária, com um percentual de 36,13% de suas conexões com velocidades superiores a 10 Mbps.

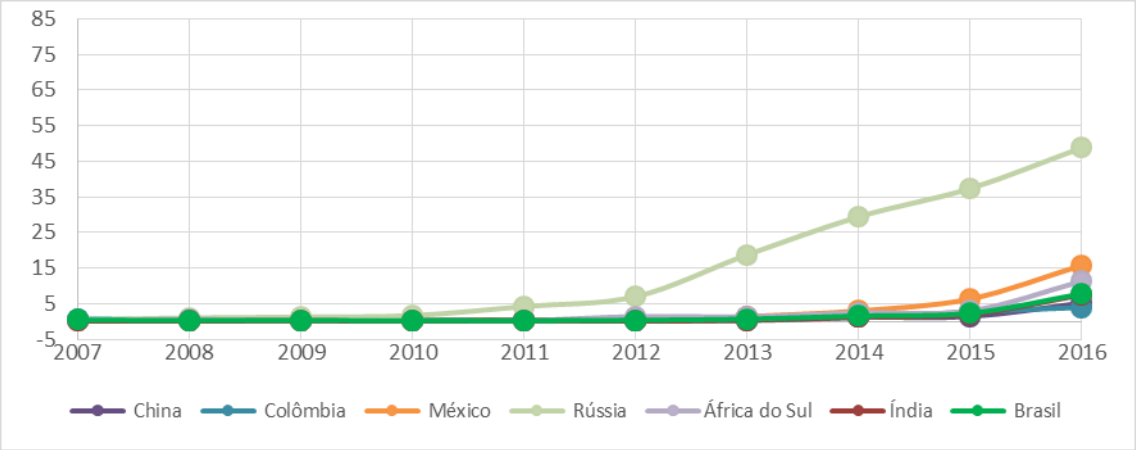
Ao analisar o Gráfico 10, que mostra os países RMA e RMB, observa-se claramente a evolução da Rússia, que se destaca dentre os demais países, ao apresentar um crescimento forte e contínuo a partir de 2011, chegando em 2016 com um percentual de 48,81% de suas conexões com velocidades superiores a 10 Mbps. Em seguida, mas com ampla diferença em relação ao desempenho da Rússia, aparecem o México, com 15,82%, e a África do Sul, com 11,35%. Já os menores percentuais relativos à quantidade de conexões que tiveram velocidades superiores a 10 Mbps nos países RMA e RMB, encontram-se, respectivamente, com a Colômbia, com apenas 4%, seguida pela Índia, com 7,56%, e o Brasil, com 7,85% de suas conexões com velocidades superiores a 10 Mbps.

GRÁFICO 9 - TAXA DA ADOÇÃO DE VELOCIDADES ACIMA DE 10 MBPS NOS PAÍSES RA (2007-2016).



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

GRÁFICO 10 - TAXA DA ADOÇÃO DE VELOCIDADES ACIMA DE 10 MBPS NOS PAÍSES RMA E RMB (2007-2016)

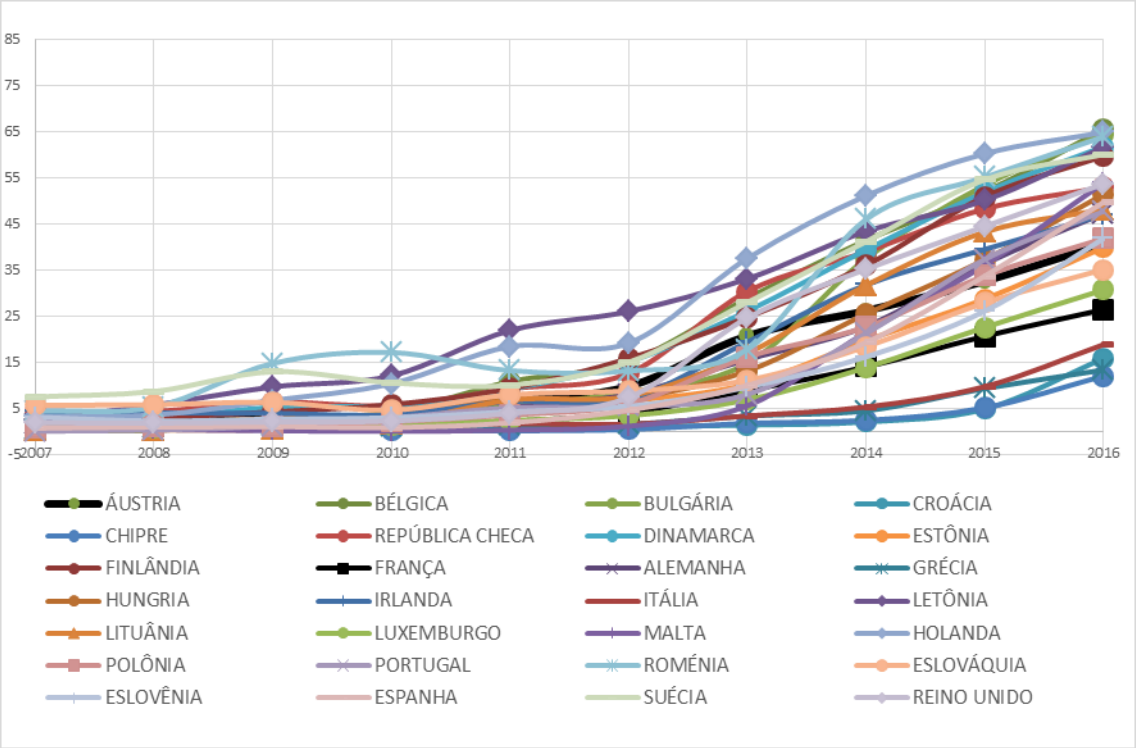


Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

O Gráfico 11, por sua vez, mostra a taxa da adoção de velocidades acima de 10 Mbps nos Estados-membros da União Europeia. Ao analisar este gráfico, percebe-se que o comportamento da União Europeia, cuja maioria dos países que a compõe pode ser classificada como RA, é muito similar ao comportamento dos outros países RA, mostrado no Gráfico 9, visto que todos os Estados-membros da União Europeia também apresentam um crescimento homogêneo. Ao analisar os Gráficos 9 e 11 em conjunto, é possível observar que o maior percentual relativo à quantidade de conexões que tiveram velocidades superiores a 10 Mbps na União Europeia, foi apresentado pela Bélgica, com 65,56%, uma diferença de mais de 15% em relação ao Japão, maior percentual dos países RA. É possível observar também que o menor percentual relativo à quantidade de conexões que tiveram velocidades superiores a 10 Mbps foi apresentado pelo Chipre, com 12,15%, uma diferença de mais de 5% em relação ao Chile, menor percentual dos países RA.

O crescimento homogêneo identificado em todos os Estados-membros pode ser explicado pela estratégia Europa 2020, e pelos objetivos estabelecidos pela União Europeia a fim de universalizar o acesso à Internet e com 100 Mbps (EUROPEAN COMMISSION, 2017a; EUROPEAN COMMISSION, 2017b).

GRÁFICO 11 - TAXA DA ADOÇÃO DE VELOCIDADES ACIMA DE 10 MBPS NOS ESTADOS-MEMBROS DA UNIÃO EUROPEIA (2007-2016)



Fonte: GONÇALVES, SETENARESKI, SHIMA, BONA, PERES e DUARTE JÚNIOR ([2017]).

6.6 UMA DISCUSSÃO SOBRE O RELACIONAMENTO ENTRE A NEUTRALIDADE DA REDE E A EVOLUÇÃO DA INFRAESTRUTURA DA INTERNET

Esta seção apresenta resultados da investigação preliminar sobre a correlação entre a regulação da Neutralidade da Rede e a evolução da Internet. Esta investigação foi motivada pelo documento da FCC (2015a), no qual está destacado que após entrarem em vigor as regras da Neutralidade da Rede de 2010, investimentos significativos e inovação revolucionária foram realizados no mercado de banda larga nos EUA. A FCC (2015a) salienta que provedores de banda larga investiram US$212 bilhões nos três anos após a adoção destas regras - de 2011 a 2013 - mais do que em qualquer período de três anos desde 2002. O referido documento permite concluir que a regulação da Neutralidade da Rede impulsiona o crescimento da Internet, mantendo a inovação e a concorrência. Concretamente, buscou-se apresentar uma discussão do impacto das regulações da Neutralidade da Rede na evolução da infraestrutura da Internet global, levando em conta os dados levantados de diversas fontes apresentados

nas seções anteriores sobre países de todo o mundo. O objetivo foi identificar o comportamento das taxas de investimento e as demais variáveis no período em que foram efetivamente estabelecidas regulações nos diversos países. Para efeitos de comparação, são também apresentados os dados correspondentes para países sem regulação.

Assim, tomando por base os dados expostos ao longo deste capítulo, que formaram o panorama da evolução da infraestrutura da Internet, em conjunto com os dados expostos no Capítulo 3, que formaram o panorama da normatização da Neutralidade da Rede, é apresentada a seguir uma discussão sobre uma possível correlação entre estes dois panoramas. Esta discussão é mostrada país a país, em ordem alfabética. Os países foram aqui classificados como tendo ou não algum tipo de normatização da Neutralidade da Rede.

A seguir são apresentados os países que possuem normatização para a Neutralidade da Rede.

Brasil - o país aprova regras da Neutralidade da Rede, em seu Marco Civil da Internet, em forma de Lei em 2014, e a regulamenta, por meio de Decreto Presidencial, em 2016. Em 2014, apresenta crescimento em seus investimentos privados e, no período entre 2014 e 2016 a sua taxa de adoção de velocidades acima de 10 Mbps cresce em torno de 4 vezes e, no mesmo período, o número de usuários da Internet aumenta em 20%. A nota IDI para o Brasil era 5,50 em 2013 e alcançou 5,99 em 2016.

Canadá – o país estabelece diretrizes para a Neutralidade da Rede em 2009; neste ano há uma queda do investimento público per capita, que havia tido seu pico no ano anterior, entretanto nos anos seguintes ao estabelecimento das diretrizes, o investimento público volta a crescer. Uma possível leitura é que foram as diretrizes que levaram a este crescimento. Os investimentos privados apresentaram crescimento contínuo desde o estabelecimento das diretrizes, chegando a seu pico em 2011. Nestes anos, a taxa de adoção de velocidades acima de 10Mbps continua em crescimento contínuo, bem como o número de usuários. Destaca-se, entretanto, que em 2009 o número de usuários da Internet do país já era elevado, acima de 27 milhões, de uma população total de 33 milhões.

Chile – a lei que regula a Neutralidade da Rede no país foi aprovada em 2010; o ano seguinte, 2011, apresentou o pico do investimento per capita tanto público quanto privado. Apesar de que a nota IDI do país ficou estável, o número de usuários da

Internet cresceu fortemente naqueles anos, bem como a taxa de adoção de velocidades acima de 10 Mbps.

Colômbia – este país aprova a sua Lei da Neutralidade da Rede em 2011. Neste mesmo ano atinge seu pico nos investimentos privados. Outro fator relevante de crescimento foi a taxa de adoção de velocidades acima de 10 Mbps que aumentou mais de 10 vezes, no período entre 2011 e 2016, enquanto o número de usuários cresceu em mais de 80% no mesmo período.

Coréia do Sul – as diretrizes para a Neutralidade da Rede neste país foram estabelecidas em 2011 e o investimento privado atingiu seu pico em 2013. Entre 2011 e 2016, a Coréia do Sul mostrou um crescimento de mais de 90% na taxa de adoção de velocidades acima de 10 Mbps. No mesmo período, sua nota IDI manteve-se praticamente estável, com crescimento inferior a 1%. Uma possível explicação para isto pode ser o fato que sua nota já era considerada alta. Em 2012 era 8,81 e em 2016 chegou a 8,84, de uma nota máxima de 10. Do mesmo modo, o número de usuários, que já era considerado alto, mais de 41 milhões em 2011, ultrapassou os 43 milhões em 2016, com um aumento inferior a 5%.

Estados Unidos – este país procura regular a Neutralidade da Rede desde 2002, lançando suas regras desde então. Ao longo deste período, é possível verificar que houve aumento dos investimentos. Conforme afirmado pelo seu órgão regulador e citado anteriormente, os provedores de banda larga investiram US$212 bilhões nos três anos após a adoção das regras de 2010, mais do que em qualquer período de três anos desde 2002. Ao analisar o aumento na taxa de adoção de velocidades acima de 10 Mbps, no período em que foram localizados dados (2007-2016), constata-se que ela aumentou mais de 18 vezes, e o número de usuários cresceu em torno de 20%.

Índia – este país, por meio de seu órgão regulador, proíbe a prática da taxa zero em 2016. Não foram localizados dados posteriores a este ano, para análise, entretanto, é possível observar, por meio dos dados obtidos entre os anos de 2007 e 2016, que a Índia obteve o pico em seu investimento privado em 2010, aumentou a sua taxa de adoção de velocidades acima de 10 Mbps em mais de 200 vezes neste período, e o número de usuários cresceu em torno de 10 vezes. Não foram localizados dados de investimento público para este país.

Japão – as diretrizes para a Neutralidade da Rede foram estabelecidas no Japão em 2007 e 2008. Ao analisar os dados obtidos (2007-2016), é possível observar que, embora este país apresente oscilações em seu investimento público, ele apresenta

crescimento em seu investimento privado, alcançando o pico em 2012. É possível observar também, que o Japão mais que triplicou a sua taxa de adoção de velocidades acima de 10 Mbps e aumentou o número de usuários em mais de 20% no mesmo período.

México – a Lei da Neutralidade da Rede foi aprovada no México em 2014. Entre 2014 e 2016 verifica-se que este país apresentou crescimento da sua taxa de adoção de velocidades acima de 10 Mbps em torno de 5 vezes, e o seu número de usuários aumentou em torno de 5%. Não foram localizados dados de investimentos a partir de 2014 para este país.

Noruega - as diretrizes para a Neutralidade da Rede na Noruega foram estabelecidas em 2009. Entre o período de 2009 e 2016, a sua taxa de adoção de velocidades acima de 10 Mbps multiplicou por 10, e o número de usuários cresceu em mais de 10%. A partir dos dados de investimentos obtidos, verifica-se que o investimento público apresentava uma leve queda em 2009 e obteve um leve aumento em 2010 e 2011. Não foram localizados dados de investimento público após 2011 e não foram localizados dados de investimento privado para este país.

União Europeia – um passo relevante dado pela União Europeia, em direção ao estabelecimento de uma única regulação para a Neutralidade da Rede a ser seguida por todos os seus Estados-membros, foi a criação do BEREC em 2009. Desde então, várias medidas foram sendo tomadas neste sentido e, em 2016, finalmente o BEREC estabelece as diretrizes a serem seguidas por todos os órgãos reguladores dos países que compõem a União Europeia. A partir da análise dos dados de investimento privado obtidos, é possível observar que a União Europeia alcançou seu pico em 2008. Não foram localizados dados de investimento público para a União Europeia. A média da nota IDI dos Estados-membros da União Europeia é 6,52, sendo que 9 Estados-membros possuem notas IDI acima de 8. São eles: Dinamarca, Estônia, Finlândia, França, Alemanha, Luxemburgo, Holanda, Suécia e Reino Unido. A taxa de adoção de velocidades acima de 10 Mbps para os Estados-membros da União Europeia apresentam um forte crescimento contínuo a partir de 2013.

A seguir são apresentados os países sem normatização da Neutralidade da Rede.

África do Sul - ao analisar os dados obtidos para este país, observa-se que a sua taxa de adoção de velocidades acima de 10 Mbps foi multiplicada em torno de 50 vezes no período em 2007 e 2016, e o número de usuários multiplicou mais de 7 vezes. Não foram localizados dados de investimento público para este país e o pico de investimento

privado ocorreu em 1999, data anterior ao início do debate mundial em torno da Neutralidade da Rede.

Austrália – a partir dos dados obtidos para a Austrália, pode-se verificar que no período compreendido entre os anos de 2007 e 2016 este país aumentou em mais de 24 vezes a sua taxa de adoção de velocidades acima de 10 Mbps. É possível observar que o número de usuários cresceu em mais de 40% e que o investimento público teve seu pico em 2011. Não foram localizados dados de investimento privado para este país.

China – os dados obtidos para a China mostram que este país atingiu seu pico de investimento privado em 2013. Não foram localizados dados de investimento público para este país. A sua taxa de adoção de velocidades acima de 10 Mbps multiplicou em quase 10 vezes no período entre 2007 e 2016, enquanto o número de usuários mais que triplicou.

Nova Zelândia – ao analisar os dados coletados para a Nova Zelândia, percebe-se que este país, entre os anos de 2007 e 2016, multiplicou em mais de 70 vezes a sua taxa de adoção de velocidades acima de 10 Mbps e que o número de usuários cresceu em mais de 40% no mesmo período. O investimento público neste país atingiu seu pico em 2010 e não foram localizados dados sobre o investimento privado.

Rússia – os dados obtidos para este país apontam que a sua taxa de adoção de velocidades acima de 10 Mbps multiplicou em mais de 100 vezes no período entre 2007 e 2016, e quase triplicou o seu número de usuários no mesmo período. O pico do investimento privado deste país ocorreu em 20111 e não foram localizados dados sobre o investimento público.

6.7. CONSIDERAÇÕES FINAIS

Embora não tenham sido localizados todos os dados de investimentos, público e privado, para todos os países analisados, e para todo o período em que perdura o debate da Neutralidade da Rede, os dados obtidos permitiram construir um panorama global, de modo a fornecer uma visão geral e embrionária sobre a evolução da infraestrutura da Internet. A investigação preliminar, proposta e apresentada neste capítulo, sobre o estabelecimento de correlação entre a Neutralidade da Rede e a evolução da infraestrutura da Internet, apontou que é prematuro alcançar um resultado conclusivo. Ao analisar os países que regularam a Neutralidade da Rede observa-se que sim, houve

evolução da infraestrutura da Internet a partir da regulação. Entretanto, ao analisar os países que não regularam a Neutralidade da Rede, mas estão iniciando o debate, como por exemplo, a Austrália e a Nova Zelândia, e países cujos governos efetuam censura, como por exemplo, a China, ou, ainda, onde a discussão sobre a Neutralidade da Rede não é uma prioridade governamental, como, por exemplo, a África do Sul, observa-se que também houve forte evolução da infraestrutura da Internet. Portanto, é prematuro afirmar que a regulação da Neutralidade da Rede representa fator determinante para a evolução da infraestrutura da Internet. Isto se deve a algumas possíveis alternativas elencadas a seguir: (i) as regulações da Neutralidade da Rede ocorreram, em sua maioria, entre o período de 2011 e 2016, restando, portanto, um curto período temporal para a análise; (ii) a análise efetuada para os países com regulação da Neutralidade da Rede se deteve nos anos posteriores à ela, enquanto que a análise para os países sem regulação da Neutralidade da Rede, foi efetuada sobre todo o período em que obteve-se dados. A razão disso foi a dificuldade em estabelecer para os países sem regulação, um marco temporal condizente com o dos países com regulação, devido a sua grande variação; (iii) alguns países, como os Estados Unidos, e ainda a União Europeia, de certo modo apostaram na regulação da Neutralidade da Rede como forma de assegurar que os ISPs mantivessem investimentos contínuos na infraestrutura da Internet e, como forma de incentivar a competitividade e a inovação. Exemplos disto são os documentos regulatórios dos Estados Unidos e da União Europeia, citados ao longo desta tese, que afirmam que a regulação da Neutralidade da Rede motivou a evolução da infraestrutura da Internet. O mesmo ocorreu com organizações como a OECD. Diante disso, é imprescindível que uma afirmação conclusiva dependa do passar de mais alguns anos para que a análise possa ser efetuada sobre os mesmos parâmetros temporais.

CAPÍTULO VII

CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo tem por objetivos apontar algumas conclusões e responder as questões de pesquisa apresentadas. E, ainda, este capítulo aponta algumas sugestões de trabalhos futuros para tratar de questões em aberto, que poderão contribuir com o avanço do tema da Neutralidade da Rede. Para atingir os objetivos aqui propostos, o capítulo é subdividido em três partes conforme segue. A Seção 7.1 traz as conclusões. A Seção 7.2 traz as respostas às questões de pesquisa apresentadas, e a Seção 7.3 aponta alguns trabalhos futuros que podem ser elaborados a partir desta tese.

7.1. CONCLUSÕES

À luz do exposto neste trabalho, é possível fazer as seguintes afirmações de forma conclusiva. O debate em torno da Neutralidade da Rede permanece. O debate da Neutralidade da Rede envolve minimamente aspectos políticos, legais, econômicos, sociais, éticos, técnicos e de competitividade e inovação. Os aspectos que envolvem o debate da Neutralidade da Rede são interdependentes. Não há previsão temporal em curto prazo, para que o debate da Neutralidade da Rede seja solucionado. Embora estas afirmações conclusivas, possam parecer óbvias depois de postas, importa sublinhar o extenso caminho percorrido na pesquisa até que pudessem ser expostas como tal. Igualmente, cumpre perpassar considerações que vieram contribuir com o embasamento destas afirmações conforme segue.

A justificativa das afirmações conclusivas. Estas afirmações devem-se basicamente a dois motivos. (i) Os opositores à Neutralidade da Rede, particularmente os ISPs, continuam exercendo pressão junto às agências reguladoras, junto a outros entes governamentais, e junto a políticos, a fim de impedir, retardar ou, até mesmo, modificar normatizações já instituídas, como ocorre nos Estados Unidos, por exemplo. (ii) Notadamente os ISPs, de acordo com seus interesses, por vezes efetuam o

gerenciamento do tráfego da Internet de forma não razoável. Este comportamento manifesta-se de várias maneiras e continua sendo questionável, visto que não é simples a sua comprovação.

É importante destacar o contexto no qual se inserem o comportamento indevido dos ISPs, e os aspectos que envolvem o debate da Neutralidade da Rede e a sua interdependência. Dois exemplos de comportamentos indevidos mostrados pelos ISPs e que, ao mesmo tempo, ilustram a dificuldade de comprovação, são o bloqueio e o estrangulamento de aplicações ou serviços. Há que se comprovar que foram feitos intencionalmente, de modo a prejudicar alguma aplicação ou serviço, por meio da diferenciação de tráfego da Internet que resultou em bloqueio ou estrangulamento. Ou, em caso contrário, há que se comprovar que foram feitos em benefício da rede e de seus usuários, como por exemplo, para evitar congestionamento, ou para auxiliar no combate a ataques. Neste contexto, a comprovação só é possível a partir de resultados fornecidos pelo uso de ferramentas desenvolvidas para este fim: detectar diferenciação de tráfego que leve a bloqueio ou a estrangulamento de aplicações ou serviços. E, ainda, é necessário que tenham sido estabelecidos parâmetros de comparação para esta comprovação, para só então ser possível assegurar com confiança os motivos que levaram os ISPs a determinado comportamento: devido ou indevido.

Neste contexto, é importante observar, não só a complexidade da fiscalização da aplicação da Neutralidade da Rede, em seus aspectos técnicos, mas também, que os aspectos políticos e legais, necessários para a normatização efetiva da Neutralidade da Rede, possuem interdependência destes aspectos técnicos para que se concretizem. Diante disso, é possível inferir que a efetividade da Neutralidade da Rede só é concreta quando a normatização é, de fato, respeitada e praticada pelos ISPs ou, em caso contrário, quando ocorre punição ou coibição. Para tanto, é necessário que haja fiscalização da Neutralidade da Rede de forma efetiva. E ela só é efetiva quando efetuada por meio da utilização de ferramentas ou mecanismos computacionais, desenvolvidos para este fim. É neste mesmo contexto que se situa também a inovação. Este aspecto se mostra interdependente dos outros aspectos na medida em que os aspectos legais, políticos e técnicos, que levam à normatização e estão contidos nela, por si só não incentivam a inovação. Dito de outra maneira, embora a normatização da Neutralidade da Rede seja baseada e inclua a inovação por parte dos ISPs em todas as camadas da rede, isto na prática nem sempre ocorre. O que se observa é que, ao promover diferenciação intencional e não razoável no gerenciamento do tráfego de suas

redes, os ISPs comportam-se de forma nociva e paliativa. O comportamento correto esperado dos ISPs, e previsto na base da Neutralidade da Rede, deveria ser o investimento na rede, a fim de ofertar mais banda, e mais, e melhores, e novos serviços. Ainda neste contexto no qual se inserem o comportamento indevido dos ISPs, e a interdependência dos aspectos que envolvem a Neutralidade da Rede, se inserem também os aspectos econômicos, sociais, éticos, e a competitividade. Um exemplo facilmente aplicável neste contexto é a prática da taxa zero.

É também imprescindível destacar o contexto no qual se insere a permanência do debate da Neutralidade da Rede, sem previsão de término em curto prazo. Em alguns países, como por exemplo, a Rússia, a Nova Zelândia, a Austrália, a África do Sul e o Quênia, o debate ainda se encontra em fase inicial ou incipiente. Nestes países, pode haver a diferenciação, a discriminação e a censura (também uma forma de diferenciação) por parte dos ISPs, sem comprovação do fato, visto que não há normatização para efeitos de comparação. Nestes países, o consumidor de serviços de rede não conta com qualquer apoio legal para exercer seu direito de escolha sobre o conteúdo que deseja acessar, caso isto não esteja ocorrendo e, tampouco, tem a quem recorrer para relatar o problema em busca de solução. E, mesmo em países que obtiveram a normatização da Neutralidade da Rede, como nos Estados–membros da União Europeia, e nos Estados Unidos, em especial neste último, o embate permanece em ebulição. Nos Estados Unidos, conforme mostrado no Capítulo 3, ocorre o questionamento, por meio de nova consulta pública, quanto às regras da Internet aberta, estipuladas somente para os ISPs, enquanto provedores de conteúdo (como, por exemplo, a Netflix (SQUEO, 2016; AMERICAN CABLE ASSOCIATION, 2016)) demonstram uma conduta irregular ao promover o seu auto estrangulamento.

Neste contexto situa-se também o Brasil. Embora a normatização no Brasil tenha ocorrida em forma de Lei e de Decreto, no país o debate também permanece e ocorrem violações da Neutralidade da Rede. Um exemplo disso é a prática da taxa zero, que no Brasil ocorre de forma explícita. A taxa zero é anunciada na mídia, ofertada livremente em forma de pacotes de dados das operadoras, como um benefício aos usuários. O apelo da oferta é de mais acesso ilimitado, por um valor monetário menor do que o valor ofertado pela concorrente. Este é um exemplo de violação que não depende de comprovação da diferenciação de tráfego em termos técnicos, visto que é declarada.

Além disso, o monitoramento de práticas que podem ser utilizadas pelos ISPs para intencionalmente violar a Neutralidade da Rede, incluindo a da taxa zero,

permanece em aberto no Brasil. Não se conhece no país nenhuma iniciativa que tenha este monitoramento como objetivo. Assim, o observatório proposto neste trabalho vem preencher esta lacuna.

7.2. QUESTÕES DE PESQUISA

A seguir são trazidas as questões de pesquisa apresentadas na introdução desta tese para serem respondidas.

QP I. Existem mecanismos computacionais, possíveis de monitorar o tráfego da rede e detectar algum tipo de violação à Neutralidade da Rede? Quais são eles?

Resposta: Sim. Existem dezenas de mecanismos computacionais, possíveis de monitorar o tráfego da rede e detectar algum tipo de violação à Neutralidade da Rede. Eles aparecem descritos nesta tese, no Capítulo IV, e em artigo de periódico elaborado para este fim. Este artigo busca sistematizar conceitos e práticas da área, trazendo dezenas de ferramentas computacionais que visam detectar diferenciação de tráfego que leva a bloqueio, estrangulamento, priorização e outras violações à Neutralidade da Rede. Este artigo relata ainda dezenas de casos reais de violações à Neutralidade da Rede.

QP II. A regulação da Neutralidade da Rede contribuiu para a evolução da Internet?

Resposta: Pela análise efetuada é possível concluir que sim, há indícios de que a Neutralidade da Rede contribuiu para a evolução da infraestrutura da Internet, de acordo com os resultados da pesquisa. Entretanto, os resultados apontam também, que é prematuro efetuar afirmações conclusivas, em especial, pelo curto período de tempo transcorrido após a maioria das regulações. Foi elaborado um artigo de periódico da área de economia que tratou desta questão. Este artigo exibe um panorama da evolução da infraestrutura da Internet no mundo e o relaciona com o panorama mundial da normatização da Neutralidade da Rede.

QP III. Existe no Brasil algum observatório que permita à sociedade acompanhar as questões relacionadas à Neutralidade da Rede, tais como o comportamento dos ISPs, quanto ao gerenciamento do tráfego efetuado em suas redes, e o comportamento da agência reguladora, quanto à fiscalização e possíveis punições aos ISPs, em caso de alguma violação à Neutralidade da Rede?

Resposta: Não**.** O resultado da pesquisa levou a dois observatórios relacionados às questões da Internet no Brasil e no mundo e também ao Marco Civil da Internet no Brasil. Entretanto, nenhum destes observatórios trata especificamente das diversas questões inerentes à Neutralidade da Rede. E nenhum deles se propõe a servir de instrumento de controle social, permitindo que a sociedade possa monitorar a fiscalização efetuada pela agência reguladora do Brasil e monitorar o comportamento dos demais agentes envolvidos, a fim de monitorar a efetividade da aplicação da Neutralidade da Rede no Brasil.

Assim, foi criado o observatório para monitorar a Neutralidade da Rede no Brasil. Isto porque ela não está sendo praticada de forma efetiva no país, mesmo após a sua normatização. A criação do ONR surge como um primeiro passo, em busca da solução deste problema. Os resultados do monitoramento, por meio do ONR, poderão subsidiar as decisões da agência reguladora do Brasil, quanto ao comportamento demonstrado pelos ISPs. Da mesma forma, os usuários finais poderão se conscientizar da importância do monitoramento do tráfego da Internet no Brasil. Finalmente, e não menos importante, por meio do ONR, os usuários finais também poderão se tornar partícipes do processo de monitoramento, auxiliando na detecção de violações, efetuadas por meio das ferramentas ali disponíveis. A participação da sociedade no ONR, neste curto período de sua existência, indica que o ONR poderá cumprir com sua missão de servir como instrumento de controle social para os vários aspectos que envolvem a Neutralidade da Rede no Brasil.

7.3. TRABALHOS FUTUROS

As sugestões para estudos futuros a fim de contribuir para o avanço da pesquisa sobre o tema da Neutralidade da Rede incluem as seguintes. Considerando a multidisciplinariedade do debate da Neutralidade da Rede, sugere-se aprofundar a pesquisa e a análise quanto a todos os aspectos envolvidos, tais como os políticos, econômicos, técnicos e outros.

Considerando a necessidade de comprovação de violações da Neutralidade da Rede por parte dos ISPs, sugere-se efetuar levantamento das iniciativas existentes, em termos mundiais, que visem monitorar o comportamento dos ISPs. Este levantamento deve ser efetuado de forma a estabelecer um panorama mundial de laboratórios e

observatórios de monitoramento da Neutralidade da Rede, a fim de propor a extensão do ONR para que integre globalmente as iniciativas existentes.

Considerando as ferramentas que visam detectar algum tipo de violação da Neutralidade da Rede, o levantamento apresentado nesta tese mostrou que, embora existam muitas ferramentas disponíveis para a detecção de alguma violação da Neutralidade da Rede, o problema é complexo e resta longe de ser equacionado. Assim, esta tese lança os fundamentos que orientam os desenvolvedores a projetar ferramentas computacionais que venham contribuir com a busca da solução para detectar qualquer tipo de manipulação indevida no tráfego da Internet, por parte dos ISPs. Para tanto, esta detecção deve cobrir a rede de ponta a ponta, e em todas as suas camadas.

Por fim, considerando a investigação preliminar sobre a contribuição da normatização da Neutralidade da Rede para a evolução da infraestrutura da Internet, os resultados apontaram para a necessidade de aprofundamento da pesquisa nesta área. À vista disso, sugere-se que este trabalho deva aguardar um período temporal mínimo de cinco anos para colher os dados necessários para a análise. Do mesmo modo, sugere-se que este trabalho amplie o número de indicadores que influenciam a evolução da infraestrutura da Internet. Desta maneira acredita-se que a análise será enriquecida e possibilitará resultados conclusivos.

REFERÊNCIAS

ABRANET - ASSOCIAÇÃO BRASILEIRA DE INTERNET. [s.l], 2017. Disponível em: <http://www.abranet.org.br> Acesso em: 26 jan 2017.

ABRANET - ASSOCIAÇÃO BRASILEIRA DE INTERNET. **Estatuto Social**. [s.l], 2009. Disponível em: <http://www.abranet.org.br/doc/estatutosocialabranet2009.pdf>. Acesso em: 26 jan 2017.

ABRINT - ASSOCIAÇÃO BRASILEIRA DE PROVEDORES DE INTERNET E TELECOMUNICAÇÕES. [s.l], 2017. Disponível em: <http://www.abrint.com.br/> Acesso em: 01 mar 2017.

ACETO, G.; PESCAPÉ, A. Internet Censorship Detection: a survey. **Computer Networks**, [s.l], n. 83, 2015. p. 381–421.

ACMA - AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA). **Six emerging trends in media and communications**. [s.l], 2014. Disponível em: <http://www.acma.gov.au/~/media/Research%20and%20Analysis/Research/pdf/Six%20emerging%20trends%20in%20media%20and%20communications_Final%20pdf.pdf > Acesso em: 16 abr 2016.

ACMA - AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA). **The Internet of Things and the ACMA's areas of focus Emerging issues in media and communications.** [s.l], 2015. Disponível em: <http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Issues%20for%20comment/pdf/Internet%20of%20Things_occasional%20paper%20pdf.pdf> Acesso em: 16 abr 2016.

ACMA - AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA).**Changes in the Australian VoIP Market.** [s.l], 2009. Disponível em: <http://www.acma.gov.au/theACMA/changes-in-the-australian-voip-market> Acesso em: 16 abr 2016.

AIDA, M.; MIYOSHI, N.; ISHIBASHI, K. A scalable and lightweight QoS monitoring technique combining passive and active approaches. **IEEE INFOCOM**, [s.l], v. 1, 2003.

AKAMAI. **Time-based trends in Internet connection speeds and adoption rates: state of the Internet**. 2017. Disponível em: <https://www.akamai.com/us/en/about/our-thinking/state-of-the-Internet-report/state-of-the-Internet-connectivity-visualization.jsp> Acesso em: 22 mai 2017

AMARAL, B. do. **Senacon implanta grupo de trabalho para monitorar neutralidade de rede**. [s.l], 2016. Disponível em: <http://convergecom.com.br/teletime/16/08/2016/senacon-implanta-grupo-de-trabalho-para-monitorar-neutralidade-de-rede>. Acesso em: 14 abr 2017.

AMERICAN CABLE ASSOCIATION. **ACA Statement On Netflix's Throttling Of Wireless Video Streaming Traffic**. [s.l], 2016. Disponível em:

<http://www.americancable.org/node/5668> Acesso em: 30 abr 2016.

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Consulta Pública nº 8/2015:** Tomada de subsídios sobre a regulamentação da neutralidade de rede, prevista no Marco Civil da Internet. Brasília, 2015c. Disponível em: <http://www.anatel.gov.br/dialogo/groups/profile/120/consulta-publica-no-82015-tomada-de-subsidios-sobre-a-regulamentacao-da-neutralidade-de-rede-prevista-no-marco-civil-da-internet> Acesso em: 23 fev 2016.

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Consumidor**. Brasília, 2014. Disponível em: <http://www.anatel.gov.br/consumidor> Acesso em: 18 mar 2017.

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Institucional**. Brasília, 2015a. Disponível em: <http://www.anatel.gov.br/institucional/institucional-menu> Acesso em: 08 fev 2017.

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Programa de Aferição de Qualidade da Banda Larga no Brasil.** [s.l], 2017. Disponível em: <http://www.brasilbandalarga.com.br/> Acesso em: 27 jan 2017

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 574, de 28 de outubro de 2011**. Aprova o Regulamento de Gestão da Qualidade do Serviço de Comunicação Multimídia (RGQ-SCM). Brasília, 2011a. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2011/57-resolucao-574> Acesso em: 02 mar 2017

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 575, de 28 de outubro de 2011**. Aprova o Regulamento de Gestão da Qualidade da Prestação do Serviço Móvel Pessoal – RGQ-SMP e altera o Regulamento do Serviço Móvel Pessoal – SMP, aprovado pela Resolução nº 477, de 7 de agosto de 2007, e alterado pelas Resoluções nº 491, de 12 de fevereiro de 2008, nº 509, de 14 de agosto de 2008, nº 564, de 20 de abril de 2011 e nº 567, de 24 de maio de 2011. Brasília, 2011b. Disponível em: <http://www.anatel.gov.br/legislacao/resolucoes/2011/68-resolucao-575> Acesso em: 02 mar 2017

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resultados das medições no quarto trimestre de 2014**. Brasília, 2015b. Disponível em: <http://www.anatel.gov.br/institucional/ultimas-noticiass/340-resultados-das-medicoes-no-quarto-trimestre-de-2014> Acesso em 27 jan 2017

ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Tomada de subsídios sobre franquia de dados na banda larga fixa**. Brasília, 2016. Disponível em: <http://www.anatel.gov.br/dialogo/groups/profile/895/tomada-de-subsidios-sobre-franquia-de-dados-na-banda-larga-fixa>. Acesso em: 19 mar 2017.

ANATEL aumenta rigor na fiscalização de operadoras de banda larga. [s.l], 2014. Disponível em: <http://www.brasil.gov.br/infraestrutura/2014/10/anatel-aumenta-rigor-na-fiscalizacao-de-operadoras-de-banda-larga> Acesso em: 18 mar 2017.

ANATEL escolhe a PwC para avaliar qualidade da banda larga no Brasil. **Valor Econômico**, [s.l], 2012. Disponível em: <http://www.valor.com.br/empresas/2547456/anatel-escolhe-pwc-para-avaliar-qualidade-da-banda-larga-no-brasil> Acesso em: 27 jan 2017

ANATEL não deve atuar como sindicato das empresas de telefonia, diz Lamachia. [s.l], 2016. Disponível em: http://www.conjur.com.br/2016-mai-03/anatel-nao-sindicato-empresas-telefonia-lamachia. Acesso em: 30 jan 2017.

ANDERSON, C. Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. **arXiv**, [s.l], 2013. Disponível em: <http://arxiv.org/pdf/1306.4361v1.pdf> Acesso em 23 set 2015.

ANDERSON, N. **FCC asks for comments on network neutrality, gets 27,000 of them**: the FCC stopped accepting reply comments on network neutrality yesterday, and. [s.l], 2007. Disponível em: <http://arstechnica.com/tech-policy/2007/07/fcc-asks-for-comments-on-network-neutrality-gets-27000-of-them> Acesso em 11 ago 2015

APLICATIVO SIMET mede qualidade da conexão em redes 3G, 4G e Wi-Fi. [s.l], 2016. Disponível em: <http://idgnow.com.br/mobilidade/2016/04/25/aplicativo-simet-mede-velocidade-de-internet-em-redes-3g-4g-e-wi-fi/>. Acesso em: 06 mar 2017.

AUSTEN, I. A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship. **The New York Times**, Nova Iorque, 2005. Disponível em: <http://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked-web-sites-and-questions-of-censorship.html?_r=0> Acesso em: 04 mar 2016.

BAJPAI, V.; SCHÖNWÄLDER, J. A Survey on Internet Performance Measurement Platforms and Related Standardization Efforts**. IEEE Communications Surveys & Tutorials**, [s.l], n. 99, abr. 2015.

BARANIUK, C. **European Parliament votes against net neutrality amendments**. Londres, 2015. Disponível em: <http://www.bbc.com/news/technology-34649067> Acesso em 23 dez 2015.

BASHKO, V. *et al*. Bonafide: a traffic shaping detection tool for mobile networks. In: IFIP/IEEE INTERNATIONAL SYMPOSIUM ON INTEGRATED NETWORK MANAGEMENT. 2013. **Anais…** Bélgica: [s.n], 2013.

BASSO, S.; FILASTÒ, A. MORFEO: MOnitoRing network connections to assess Freedom. **Internet Science – EU, Open Call Project**, [s.l], 2015, 12 p. Disponível em: <http://www.internet-science.eu/sites/eins/files/biblio/MORFEO_D2.1.pdf> Acesso em: 12 out 2015.

BASSO, S.; MEO, M.; DE MARTIN, J. C. Strengthening Measurements from the Edges: Application-level Packet Loss Rate Estimation. **SIGCOMM Computer Communication Review**, [s.l], v. 43, n. 3, 2013.

BASSO, S.; SERVETTI, A.; DE MARTIN, J. C. The network neutrality bot architecture: A preliminary approach for self-monitoring of Internet access QoS. In: COMPUTERS AND COMMUNICATIONS. 2011. **Anais…** [s.l: s.n]. 2011.

BEREC - BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS. **BEREC Guidelines for quality of service in the scope of net neutrality**. [s.l], 2012a. 67 p. Disponível em: <http://berec.europa.eu/eng/document register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality> Acesso em: 19 mai 2015.

BEREC - BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS. **BEREC Guidelines on Net Neutrality and Transparency**: best practices and recommended approaches. [s.l], 2011. 64 p. Disponível em: <http://berec.europa.eu/files/news/consultation_draft_ guidelines.pdf.> Acesso em: 15 mai 2015.

BEREC - BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS. **BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules**. [s.l], 2016a. Disponível em: <http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules>. Acesso em: 03 jan 2017.

BEREC - BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS. **BEREC launches Net Neutrality Guidelines**. [s.l], 2016b. Disponível em: <http://berec.europa.eu/eng/news_and_publications/whats_new/3958-berec-launches-net-neutrality-guidelines >. Acesso em 03 jan 2017

BEREC - BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS. **Summary of BEREC positions on net neutrality**. [s.l], 2012b. Disponível em: <http://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/1128-summary-of-berec-positions-on-net-neutrality> Acesso em 11 jun 2015.

BERNERS-LEE, T. Long Live the Web. **Scientific American**, [s.l], v. 303, n. 6, 2010. p. 80-85.

BERNERS-LEE, T.; FISCHETTI, M. **Weaving the web**: the original design of the world wide web by its inventor. New York: HarperCollins, 2000. 243p.

BEVERLY, R.; BAUER, S.; BERGER, A. The Internet is Not a Big Truck: Toward Quantifying Network Neutrality**.** In: International Conference on Passive and Active Network Measurement (PAM). 2007. **Anais…** Springer-Verlag: [s.n], 2007.

BISCHOF, Z. S. *et al*. Crowdsourcing ISP Characterization to the Network Edge. In: SIGCOMM WORKSHOP ON MEASUREMENTS UP THE STACK (W-MUST).2011. **Anais…** [s.l]: ACM. 2011.

BISCHOF, Z. S., OTTO, J. S.; BUSTAMANTE, F. E. Up, Down and Around the Stack: ISP Characterization from Network Intensive Applications. **SIGCOMM Computer Communication Review**, [s.l], v. 42, n. 4, 2012.

BOECHAT, Lucas. **Provedores de Internet no Brasil**. [s.l], 2015. Disponível em: <https://techinbrazil.com.br/provedores-de-internet-no-brasil> Acesso em: 07 mar 2017.

BOTTA, A.; DAINOTTI, A.; PESCAPÉ, A. A Tool for the Generation of Realistic Network Workload for Emerging Networking Scenarios. **Computer Networks**, [s.l], v. 56, n. 15, 2012.

BRASIL. Câmara dos Deputados e Senado Federal. **Emenda Constitucional Nº 8, de 1995**. Altera o inciso XI e a alínea "a" do inciso XII do art. 21 da Constituição Federal. Brasília, 1995. Disponível em: <http://www2.camara.leg.br/legin/fed/emecon/1995/emendaconstitucional-8-15-agosto-1995-354956-publicacaooriginal-1-pl.html> Acesso em: 08 fev 2017.

BRASIL. Câmara dos Deputados. **Lei nº 8.884, de 11 de junho de 1994**. Transforma o Conselho Administrativo de Defesa Econômica (CADE) em Autarquia, dispõe sobre a prevenção e a repressão às infrações contra a ordem econômica e dá outras providências. Brasília, 1994. Disponível em: <http://www2.camara.leg.br/legin/fed/lei/1994/lei-8884-11-junho-1994-349808-norma-pl.html>. Acesso em 09 fev 2017

BRASIL. CÂMARA DOS DEPUTADOS. **PL 2126/2011**. Brasília, 2011a. Disponível em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255> Acesso em: 19 fev 2016.

BRASIL. Casa Civil. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 27 fev 2017.

BRASIL. Casa Civil. Decreto Nº 4.829, de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Brasília, 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm> Acesso em: 27 fev 2017.

BRASIL. Casa Civil. **Decreto nº 7.738, de 28 de maio de 2012**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Conselho Administrativo de Defesa Econômica – CADE; remaneja cargos em comissão e funções de confiança; altera os Decretos no 6.061, de 15 de março de 2007, no 2.181, de 20 de março de 1997, e no 1.306, de 9 de novembro de 1994. Brasília, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7738.htm> Acesso em 09 fev 2017

BRASIL. Casa Civil. **Lei 9.472**, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Brasília, 1997b. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9472.htm> Acesso em: 08 fev 2017.

BRASIL. Casa Civil. **Lei nº 12.529, de 30 de novembro de 2011**. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei no 8.137, de 27 de dezembro de 1990, o Decreto-Lei no 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei no 7.347, de 24 de julho de 1985; revoga dispositivos da Lei no 8.884, de 11 de junho de 1994, e a Lei no 9.781, de 19 de janeiro de 1999; e dá outras providências. Brasília, 2011c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12529.htm> Acesso em 09 fev 2017

BRASIL. Congresso Nacional**. PLC 79/2016**. Altera as Leis nºs 9.472, de 16 de julho de 1997, para permitir a adaptação da modalidade de outorga de serviço de telecomunicações de concessão para autorização, e 9.998, de 17 de agosto de 2000; e dá outras providências. Brasília, 2016b. Disponível em: <file:///C:/Users/BC-11/Downloads/sf-sistema-sedol2-id-documento-composto-60931%20(1).pdf.

BRASIL. **Decreto nº 2.181, de 20 de março de 1997**. Dispõe sobre a organização do Sistema Nacional de Defesa do Consumidor - SNDC, estabelece as normas gerais de aplicação das sanções administrativas previstas na Lei nº 8.078, de 11 de setembro de 1990, revoga o Decreto Nº 861, de 9 julho de 1993, e dá outras providências. Brasília, 1997a. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d2181.htm> Acesso em 09 fev 2017

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 02 mai 2015.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providência. Brasília, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm> Acesso em 09 fev 2017

BRASIL. **Marco civil da internet**: seus direitos e deveres em discussão. [s.l, 2016a]. Disponível em: <http://culturadigital.br/marcocivil/>Acesso em: 22 jan 2016.

BRASIL. Ministério Da Ciência, Tecnologia, Inovações E Comunicações. **Nota**: Ministério garante que não mudará o modelo atual de planos de banda larga fixa. Brasília, 2017b. Disponível em:<http://www.mcti.gov.br/pagina-noticia/-/asset_publisher/IqV53KMvD5rY/content/nota-ministerio-garante-que-nao-mudara-o-modelo-atual-de-planos-de-banda-larga-fixa;jsessionid=4FC1DE4A6031FEEE4DC0BBB652DC01A8.columba?p_p_auth=XM1vGxdL&_101_INSTANCE_IqV53KMvD5rY_redirect=%2F>. Acesso em: 08 abr 2017.

BRASIL. MINISTÉRIO DA JUSTIÇA. **Marco Civil da Internet**: 1ª e 2ª fases. [s.l, 2016b]. Disponível em <http://pensando.mj.gov.br/marcocivil> Acesso em : 23 fev 2016.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. **Nota Técnica Nº 02/2015**: Análise do Projeto "Internet.org" e o Princípio da Neutralidade da Rede. [s.l, 2015]. Disponível em: <http://convergenciadigital.uol.com.br/inf/nota-tecnica_02-2015.pdf> Acesso em: 23 fev 2016.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Decreto nº 8.771**, de 11 de maio de 2016: Regulamenta a Lei no 12.965, de 23 de abril de 2014. [s.l], 2016a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm> Acesso em: 19 mai 2016

BRASIL. PRESIDÊNCIA DA REPÚBLICA. **Mensagem Presidencial nº 326/2011**. 2011b. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=D272A93F3D42F351AE84E34549D702EC.node2?codteor=913021&filename=Tramitacao-PL+2126/2011> Acesso em: 22 fev 2016.

BRASIL. SENADO FEDERAL. **Consulta Pública PLC 79/2016**: Projeto de Lei da Câmara nº 79 de 2016. Brasília, 2016c. Disponível em: <https://www12.senado.leg.br/ecidadania/visualizacaomateria?id=127688>. Acesso em: 08 abr 2017.

BRASIL. SENADO FEDERAL. **Projeto de lei do Senado Nº 174, de 2016**. Ementa: Insere o inciso XIV no art. 7º da Lei 12.965, de 23 de abril de 2014, para vedar a implementação de franquia limitada de consumo nos planos de internet banda larga fixa. Autoria: Senador Ricardo Ferraço. Brasília, 2017a. Disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/125599> Acesso em: 08 abr 2017.

BRASIL. Senado Federal. **Senado aprova projeto que proíbe limitação de dados na internet fixa**. Brasília, 2017c. Disponível em: http://www12.senado.leg.br/noticias/materias/2017/03/15/senado-aprova-projeto-que-proibe-limitacao-de-dados-na-internet-fixa. Acesso em: 08 abr 2017.

BRITTO, T. A. de. **Neutralidade Redes: uma análise de mercado de dois lados**. [s.l], 2015. Disponível em: <http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/dee-publicacoes-anexos/neutralidade_redes_uma_analise_mercado_dois_lados_tatiana_alessio_de_britto.pdf> Acesso em 25 mar 2017

BRODKIN, J. **Cable group**: Net neutrality rules for Netflix! (but not for us): Netflix shouldn't be allowed to throttle itself, small cable companies tell FCC. [s.l], 2016a. Disponível em: <http://arstechnica.com/business/2016/03/cable-group-net-neutrality-rules-for-netflix-but-not-for-us> Acesso em: 30 abr 2016.

BRODKIN, J. **House votes to undermine net neutrality rules, and ISPs cheer Vote to ban "rate regulation" would limit FCC's consumer protection powers**. [s.l], 2016b. Disponível em: <http://arstechnica.com/tech-policy/2016/04/house-passes-gop-bill-to-undermine-fccs-net-neutrality-authority> Acesso em: 28 abr 2016.

BRODKIN, J. **Netflix performance on Verizon and Comcast has been dropping for months**: latest Netflix data shows some ISPs struggling, while Google Fiber soars. [s.l], 2014. Disponível em: <http://arstechnica.com/information-technology/2014/02/netflix-performance-on-verizon-and-comcast-has-been-dropping-for-months> Acesso em: 06 nov 2015.

BRODKIN, J. **Netflix should be investigated for throttling itself, FCC Republican says**: Michael O'Rielly: The FCC, FTC, and Congress should all investigate. [s.l], 2016c. Disponível em: <http://arstechnica.com/business/2016/03/netflix-should-be-investigated-for-throttling-itself-fcc-republican-says> Acesso em: 28 abr 2016.

BT heavily throttling BBC, all video. [s.l], 2009. Disponível em**<**http://fastnetnews.com/dslprime/42-d/1758-bt-heavily-throttling-bbc-all-video>Acesso em: 24 set 2015.

BUSTOS-JIMÉNEZ, J. *et al*. Adkintun: SLA monitoring of ISP broadband offerings. In: ADVANCED INFORMATION NETWORKING AND APPLICATIONS WORKSHOPS, 2013. **Anais…** [s.l: s.n], 2013a. p.1445-1449.

BUSTOS-JIMÉNEZ, J. *et al*. How Adkintun Mobile measured the world. In:ACM CONFERENCE ON PERVASIVE AND UBIQUITOUS COMPUTING ADJUNCT PUBLICATION, 2013b. **Anais…**New York, NY, USA: [s.n], 2013b. p. 1457-1462.

BUSTOS-JIMÉNEZ, J.; FUENZALIDA, C. All packets are equal, but some are more equal than others. In: LANC, 2014. **Anais…** Montevideo, Uruguay: [s.n], 18-19 set. 2014. Disponível em: <http://dx.doi.org/10.1145/2684083.2684088> Acesso em: 22 jan 2015.

CADE - CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. [s.l, 2017]. Disponível em: <http://www.cade.gov.br> Acesso em 02 jan 2017

CADE - CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. Relatório de Gestão 2015. [s.l], 2016. Disponível em: file:///C:/Users/BC-11/Downloads/Relat%C3%B3rio%20de%20Gest%C3%A3o%202015%20-%20Final.pdf. Acesso em 25 mar 2017

CALLADO, A. et al. A Survey on Internet Traffic Identification. **IEEE Communications Surveys & Tutorials**, [s.l], v. 11, n. 3, 2009.p.37-52.

CAMPBELL, P. S. **Public Interest Groups Urge FCC Action Against Zero-Rating**. [s.l], 2016. Disponível em: <http://www.lexology.com/library/detail.aspx?g=e4fbf6ad-03f4-4a04-83c9-f4220c6dea26> Acesso em 01 mai 2016.

CARBONE, M.; RIZZO, L. Dummynet Revisited. **SIGCOMM Computer Communication**

Review, [s.l], v. 40, n.2, 2010.

CEPTRO - CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIAS DE REDES E OPERAÇÕES. [s.l], 2017. Disponível em: <http://www.ceptro.br/> Acesso em 02 jan 2017.

CERT - CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA. [s.l], 2017. Disponível em: <http://www.cert.br/> Acesso em 02 jan 2017.

CETIC - CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. [s.l], 2017. Disponível em: <http://www.cetic.br/>. Acesso em 02 jan 2017.

CEWEB - CENTRO DE ESTUDOS SOBRE TECNOLOGIAS WEB. [s.l], 2017. Disponível em: <http://ceweb.br/> Acesso em 02 jan 2017.

CGI - COMITÊ GESTOR DA INTERNET NO BRASIL. [s.l], 2017. Disponível em: <http://www.cgi.br/> Acesso em 02 jan 2017.

CGI - COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Provedores 2014: pesquisa sobre o setor de provimento de serviços de internet no Brasil. [s.l], 2016b. Disponível em: <http://www.cgi.br/media/docs/publicacoes/2/TIC_Provedores_2014_livro_eletronico.pdf> Acesso em: 28 fev 2017.

CGI - COMITÊ GESTOR DA INTERNET NO BRASIL. Ata da Reunião de 05 de junho de 2009. [s.l], 2009b. Disponível em: <http://www.cgi.br/reunioes/ata/2009/06> Acesso em: 22 fev 2016.

CGI - COMITÊ GESTOR DA INTERNET NO BRASIL. CGI.br apresenta contribuição para a regulamentação do Marco Civil da Internet. [s.l], 2015. Disponível em <http://www.cgi.br/noticia/releases/cgi-br-apresenta-contribuicao-para-a-regulamentacao-do-marco-civil-da-internet/> Acesso em: 23 fev 2016.

CGI - COMITÊ GESTOR DA INTERNET NO BRASIL. CGI.br cria grupo de trabalho sobre franquia de dados na banda larga fixa. [s.l], 2016a. Disponível em <http://cgi.br/noticia/notas/cgi-br-cria-grupo-de-trabalho-sobre-franquia-de-dados-na-banda-larga-fixa> Acesso em: 01 mai 2016.

CGI.br - COMITÊ GESTOR DA INTERNET NO BRASIL. **Resolução CGI.br/RES/2009/003/P.** São Paulo, 2009a. Disponível em: <https://www. CGI.br/resolucoes/documento/2009/CGI.br_Resolucao_2009_003. pdf> Acesso em: 05 mai 2015

CHENG, Y. C. *et al*. Monkey See, Monkey Do: A Tool for TCP Tracing and Replaying. In: USENIX, 4., 2004. **Anais…** [s.l: s.n]. 27/jun.-2/jul. 2004.

CHILE. **Lei n. 20453**, de 18 de agosto de 2010. Consagra el principio de neutralidad en la red para los consumidores y usuarios de internet. [s.l], 2010. Disponível em

<http://www.leychile.cl/N?i=1016570&f=2010-08-26&p=>Acesso em: 02/05/2015.

COATES, A. *et al*. Internet tomography. **IEEE Signal Processing Magazine**, [s.l], v. 19, n.3, 2002.

COLÔMBIA. CONGRESO NACIONAL. **Ley 1.450 de 2011**: por lacual se expideelPlan Nacional de Desarrollo, 2010-2014. [s.l], 2011a. Disponível em <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101> Acesso em: 01 mai 2016.

COLÔMBIA. LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES. **Resolución 3.502 de 2011**: por la cual se establecen las condiciones regulatorias relativas a la neutralidad en Internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011. [s.l], 2011b. Disponível em: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45061> Acesso em: 01 mai 2016.

COMCOM - COMMERCE COMMISSION OF NEW ZEALAND. **High speed broadband services demand side study**: Final report. Project no. 13.07/12813. [s.l], 2012. Disponível em: <http://www.comcom.govt.nz/regulated-industries/telecommunications/monitoring-reports-and-studies/studies/high-speed-broadband-services-demand-side-study/> Acesso em: 12 abr 2016.

COMCOM - COMMERCE COMMISSION OF NEW ZEALAND. **Media Releases**. [s.l], 2011. Disponível em: <http://www.comcom.govt.nz/the-commission/media-centre/media-releases/2011/commerce-commission-releases-issues-paper-on-high-speed-broadband-demand-side-study> Acesso em: 12 abr 2016.

COMER, D. E. **Interligação em Redescom TCP/IP.** 6. Ed. [s.l]: Editora Pearson, 2015.

COMMUNICATIONS AUTHORITY OF KENYA. **Home**. [s.l], 2016. Disponível em: <http://www.ca.go.ke> Acesso em: 23 abr 2016.

COSTA, M. da. Era da banda larga fixa ilimitada acabou, diz presidente da Anatel. **Folha de São Paulo**, São Paulo, 2016. Disponível em: http://www1.folha.uol.com.br/mercado/2016/04/1762387-era-da-banda-larga-fixa-ilimitada-acabou-diz-presidente-da-anatel.shtml. Acesso em: 30 jan 2017.

CROWCROFT, J. Net Neutrality: the technical side of the debate – a white paper. **Computer Communication Review**, [s.l], v. 37, n. 1, 2007, p. 49-56. Disponivel em: <http://dx.doi.org/10.1145/1198255.1198263> Acesso em: 22 jan 2015.

CRTC - CANADIAN RADIO-TELEVISION AND TELECOMMUNICATIONS COMMISSION. **Telecom Regulatory Policy CRTC 2009-657**: review of the Internet traffic management practices of Internet service providers. Ottawa, 2009. Disponível em: <http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm> Acesso em 07 mai 2015.

DEEB, K.; O'BRIEN, S. P.; WEINER, Matthew E. A Survey on Network Neutrality: a new form of discrimination based on network profiling. **Global Telecommunications**

Conference, [s.l], 2008, p. 1-6.

DHAWAN, M. *et al*. Fathom: A Browser-based Network Measurement Platform. In: ACM CONFERENCE ON INTERNET MEASUREMENT CONFERENCE. 2012. **Anais…** [s.l]: ACM. 2012.

DICIONÁRIO do Aurélio. [s.l], 2016. Disponível em: <https://dicionariodoaurelio.com/observatorio>. Acesso em: 30 out 2016.

DISCHINGER, M. *et al*. Characterizing Residential Broadband Networks. In: SIGCOMM CONFERENCE ON INTERNET MEASUREMENT. 2007. **Anais…** [s.l]: ACM. 2007.

DISCHINGER, M. *et al*. Detecting Bittorrent Blocking. In: SIGCOMM CONFERENCE ON INTERNET MEASUREMENT. 8. 2008. **Anais…** [s.l]: Association for Computing Machinery (ACM), 2008.

DISCHINGER, M. *et al*. **Glasnot**: enabling end users to detect traffic differentiation. [s.l], 2010. Disponível em: <http://www.mpi-sws.org/~gummadi/papers/glasnost.pdf> Acesso em: 30 jan. 2015.

DONNET, B.; FRIEDMAN, T. Internet topology discovery: a survey. **IEEE Communications Surveys & Tutorials**, [s.l], v. 9, n. 4, 2007.p.56-69.

DOVROLIS, C. *et al*. Measurement Lab: Overview and an Invitation to the Research Community. **SIGCOMM Computer Communication Review**, [s.l], v. 40, n.3, 2010.

DREIER, T. **Comcast Hit With FCC Complaint Over Net Neutrality Violations Public Knowledge has filed a complaint alleging that Comcast is violating its own merger agreement and the FCC's Open Internet rules**. [s.l], 2016. Disponível em: <http://www.streamingmedia.com/Articles/News/Online-Video-News/Comcast-Hit-With-FCC-Complaint-Over-Net-Neutrality-Violations-109609.aspx> Acesso em: 07 mar 2016.

ECONOMIDES, Nicholas; TAG, Joacim. Network neutrality on the Internet: A two-sided market analysis. **InformationEconomicsandPolicy**, n. 24, 2012, p. 91–104. Disponível em: <10. 1016/j. infoecopol. 2012. 01. 001> Acesso em: 20 jun 2017

ESNAASHARI, S. **Invisible Barriers**: Identifying restrictions affecting New Zealanders' access to the Internet. 206 f. Tese, Victoria University of Wellington, 2014. Disponível em: <http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/3263/thesis.pdf?sequence=2> Acesso em: 05 ago 2015

EU wants to thank everyone who participated in this outstanding effort to protect net neutrality in Europe and keep the Internet free and open! Internet wins, thank you! [s.l], 2016. Disponível em: <https://www.savetheinternet.eu/>. Acesso em 03 jan 2017.

EUROPEAN COMMISSION. **Broadband Strategy & Policy**.[s.l], 2017b. Disponível em:

<https://ec.europa.eu/digital-single-market/en/broadband-strategy-policy> Acesso em: 06 jun 2017.

EUROPEAN COMMISSION. **Digital Agenda**: Commission launches consultation on net neutrality. [s.l], 2010. Disponível em: <http://europa.eu/rapid/press-release_IP-10-860_en.htm?locale=en> Acesso em: 07 mai 2015.

EUROPEAN COMMISSION. **EU Telecoms Reform**: 12 reforms to pave way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens. [s.l], 2009. Disponível em: <http://europa.eu/rapid/press-release_MEMO-09-513_en.htm?locale=en> Acesso em: 07 mai 2015

EUROPEAN COMMISSION. **Europe 2020 strategy**.[s.l], 2017a.Disponível em: <https://ec.europa.eu/digital-single-market/en/europe-2020-strategy> Acesso em: 06 jun 2017.

EUROPEAN COMMISSION. **Implementation of the EU regulatory framework for electronic communications**. [s.l], 2014. Disponível em: <file:///C:/Users/BC-11/Downloads/2014CompleteImplementationReport%20(1).pdf> Acesso em: 26 mai 2015

EUROPEAN COMMISSION. **Roaming charges and open Internet: questions and answers.** [s.l], 2015. Disponível em: <file:///C:/Users/BC-11/Downloads/MEMO-15-5275_EN.pdf> Acesso em: 14 jul 2015.

EUROPEAN COMMISSION. **The open internet and Net(work) Neutrality in Europe**. [s.l], 2011. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52011DC0222> Acesso em: 07 mai 2015.

EUROPEAN PARLIAMENT**. Directive 2009/140/EC.** [s.l], 2009. Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF> Acesso em: 19 mai 2015.

EUROPEAN PARLIAMENT. **The open internet and net neutrality in Europe.** [s.l], 2011. Disponível em: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1431032441362&uri=CELEX:52011IP0511> Acesso em: 07 mai 2015.

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **Complying with the antimonopoly law secures the main principles of network neutrality**. [s.l], 2015a. Disponível em: <http://en.fas.gov.ru/news/news_34196.html> Acesso em 29 mai 2015.

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **Creating equal conditions on the market of Internet services**. [s.l], 2016. Disponível em: <http://en.fas.gov.ru/press-center/news/detail.html?id=44823> Acesso em: 01 mai 2016.

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **Results of the second meeting of the Working group on implementing the network neutrality principles**. [s.l], 2015b. Disponível em: <http://en.fas.gov.ru/press-center/news/detail.html?id=44277> Acesso em: 08 jan 2016.

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **The Government of the Russian Federation approved the Action Plan for developing competition in telecommunications**. [s.l], 2014. Disponível em: <http://en.fas.gov.ru/news/news_33513.html> Acesso em: 19 jun 2015.

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **The outcome of the third meeting of the Working Group on implementing network neutrality principles**. [s.l], 2015d. Disponível em: <http://en.fas.gov.ru/press-center/news/detail.html?id=44325> Acesso em: 08 jan 2016

FAS – FEDERAL ANTIMONOPOLY SERVICE OF THE RUSSIAN FEDERATION. **The results of the first session of the Working Group on implementing the principles of network neutrality**. [s.l], 2015c. Disponível em: <http://en.fas.gov.ru/news/news_34354.html> Acesso em: 29 mai 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Chairman Pai statement on free data programs**. [s.l], 2017a. Disponível em: <https://www.fcc.gov/document/statement-chairman-pai-free-data-programs>. Acesso em: 07 fev 2017.

FCC – FEDERAL COMMUNICATIONS COMMISSION. Chairman Pai statement on revoking midnight regulations.[s.l], 2017b. Disponível em: <https://www.fcc.gov/document/statement-chairman-pai-revoking-midnight-regulations>. Acesso em: 07 fev 2017.

FCC – FEDERAL COMMUNICATIONS COMMISSION. **Fact Sheet**: Restoring Internet Freedom. Notice of Proposed Rulemaking – WC Docket No. 17-108.[s.l], 2017c. Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-344614A1.pdf. Acesso em: 29 mai 2017.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC 05-150. Report and order and notice of proposed rulemaking.** [s.l], 2005b. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-150A1.pdf> Acesso em: 12 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC 05-151. Policy statement.** [s.l], 2005a. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf: Acesso em: 12 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC 09-93. Notice of Proposed Rulemaking.** [s.l], 2009. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf> Acesso em: 13 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC 10-201. Report And Order.** [s.l], 2010. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf> Acesso em: 17 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC 14-61. Notice of Proposed Rulemaking.** [s.l], 2014a. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1.pdf> Acesso em: 20 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC classifies cable modem service as information service.** [s.l], 2002. Disponível em: <http://transition.fcc.gov/Bureaus/Cable/News_Releases/2002/nrcb0201.html>. Acesso em: 28 abr 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Measuring Broadband America - July 2012:** A Report on Consumer Wireline Broadband Performance in the U.S. 2012. [s.l], 2012a. Disponível em: <https://www.fcc.gov/measuring-broadband-america/2012/july> Acesso em: 13 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Measuring Broadband America.** [s.l], 2015a. Disponível em: <http://www.fcc.gov/measuring-broadband-america> Acesso em: 13 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Open Internet**: Maintaining a Fast, Fair, and Open Internet. [s.l], 2015b. Disponível em: <https://www.fcc.gov/openinternet>Acesso em: 02 mai 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Opposition of Comcast corporation.** [s.l], 2016a. Disponível em: <http://apps.fcc.gov/ecfs/document/view?id=60001533897> Acesso em: 29 abr 2016.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Petition for the Federal Communications Commission to Enforce Merger Conditions and its Policies.** [s.l], 2016b. Disponível em: <http://apps.fcc.gov/ecfs/document/view;NEWECFSSESSION=3VtyWwrHnw6hsLjgRFlFYvm1zH99QtYQQMrcRhZJnWqpyXrJhJfg!1749169674!-1651119231?id=60001526808> Acesso em: 29 abr 2016.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Public Notice. DA 12-235.FCC Announces Commencement of 2012 Measuring Broadband America Performance Study of Residential Broadband Service in the United States.** [s.l], 2012b. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DA-12-235A1.pdf> Acesso em: 13 ago 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Public Notice**: **DA 14-211**. New docket established to address open internet remand GN Docket No. 14-28. [s.l], 2014b. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DA-14-211A1.pdf> Acesso em: 30 jul 2015

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Remarks of FCC Chairman Tom Wheeler.** [s.l], 2016c. Disponível em: <http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0411/DOC-338806A1.pdf> Acesso em: 01 mai 2016.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Report and Order on Remand, Declaratory Ruling, and Order**. FCC 15-24. [s.l], 2015c. Disponível em: <http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf> Acesso em: 02 mai 2015.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **Statement of commissioner Michael O'Rielly on conclusion of zero rating inquiries**. [s.l], 2017d. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DOC-343340A1.pdf>. Acesso em: 07 fev 2017.

FCC - FEDERAL COMMUNICATIONS COMMISSION. **FCC Takes Action to Restore Internet Freedom**. [s.l], 2017e. Disponível em: <https://www.fcc.gov/document/fcc-takes-action-restore-internet-freedom> Acesso em: 18 dez 2017.

FILASTÒ, A.; APPELBAUM, J. OONI: Open Observatory of Network Interference. In: USENIX SECURITY SYMPOSIUM, 21., 2012. **Anais…** [s.l: s.n], 8-10 ago. 2012. Disponível em: <https://www.usenix.org/ system/files/conference/foci12/foci12-final12.pdf> Acesso em: 08 out 2015.

FINLEY, K. **Net Neutrality Is in More Danger Than Ever**. [s.l], 2016. Disponível em: <http://www.wired.com/2016/03/despite-fcc-net-neutrality-danger-ever> Acesso em: 24 abr 2016.

FUNG, B. The FCC just voted to repeal its net neutrality rules, in a sweeping act of deregulation. **The Washington Post**, 2017. Disponível em: <https://www.washingtonpost.com/news/the-switch/wp/2017/12/14/the-fcc-is-expected-to-repeal-its-net-neutrality-rules-today-in-a-sweeping-act-of-deregulation/?utm_term=.dfe8cff29021> Acesso em 18 dez 2017.

GANLEY, P.; ALLGROVE, B. Net(work) Neutrality: a user's guide. **Computer Law & Security Report**, [s.l], v.22, 2006. p. 454-463.

GOEL, U. *et al*. Survey of End-to-End Mobile Network Measurement Testbeds, Tools, and Services. **IEEE Communications Surveys & Tutorials**, [s.l], n. 99, out. 2015.

GOMES, J. V. *et al*. Detection and Classification of Peer-to-Peer Traffic:a survey**. ACM Computing Surveys**, [s.l], v. 45, n. 3, jun 2013, p.1-40.

GONÇALVES, Lucas Henrique; SETENARESKI, Ligia Eliana; SHIMA, Walter Tadahiro; BONA, Luis Carlos Erpen de; PERES, Leticia Mara; DUARTE JÚNIOR, Elias Procópio. Impactos da regulação da Neutralidade da Rede na evolução da infraestrutura da Internet: uma investigação preliminar da correlação. ([2017]). **Submetido para a Revista de Economia Política, em 12 dez 2017**.

GOOGLE. **Is my ISP throttling Youtube?** [s.l], 2013. Disponível em: <https://productforums.google.com/forum/#!topic/youtube/fUig1oN9ce4> Acesso em: 27 mar 2015.

GOVERNO pretende “presentear” empresas de telefonia com milhões em patrimônio e perdão de dívidas. [s.l], 2016. Disponível em: <http://noticias.r7.com/jornal-da-record/videos/governo-pretende-presentear-empresas-de-telefonia-com-milhoes-em-patrimonio-e-perdao-de-dividas-20122016>. Acesso em: 08 abr 2017.

GREENLAND, S.; ROBINS, J. M.; PEARL, J. Confounding and Collapsibility in Causal Inference. **Statistical Science**, [s.l], v. 14, n. 1, 1999.

GROSSMANN, L. O.; COSTA, P. **MCTIC defende flexibilização do Marco Civil da Internet**. [s.l], 2016. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44084&sid=8>. Acesso em: 13 jan 2017.

GROSSMANN, L. O.; QUEIROZ, L. **Dilma recebe Decreto do Marco Civil que proíbe ‘zero rating’**. [s.l], 2016. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=42346&sid=4> Acesso em: 06 mai 2016.

GROSSMANN, L. O.; QUEIROZ, L. **Price Water house Coopers fará medição "oficial" da qualidade da Internet**. [s.l], 2012. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=*site*&infoid=29355&sid=4> Acesso em: 15 mar 2017.

H.R. 2666 (114th): no rate regulation of broadband internet access act. [s.l], 2017. Disponível em: <https://www.govtrack.us/congress/bills/114/hr2666>. Acesso em: 21 abr 2017.

HAHN, R.; WALLSTEN, S.The economics of net neutrality.The Berkeley Electronic Press, Economists’ Voice, 2006. Disponível em: <https://server1. tepper. cmu. edu/ecommerce/economics%20of%20net%20neutrality. pdf>Acesso em: 22 abr 2017

HAKOM. [s.l], 2015. Disponível em: <http://www.hakom.hr/default.aspx?id=1144>Acesso em: 20 mar 2015

HILL, L.; MARTINEZ, A. R. Africa internet access more important for Africa than net neutrality, which is a ‘first world’ problem. **Mail & Guardian Africa**, [s.l], 2016 . Disponível em: <http://mgafrica.com/article/2016-02-24-africa-internet-access-more-important-for-africa-than-net-neutrality-which-is-a-first-world-problem> Acesso em: 11 abr 2016.

HOFSTEDE, R. *et al*. Flow Monitoring Explained: from packet capture to data analysis with NetFlow and IPFIX. **Communication Surveys & Tutorials**, [s.l], v. 16, n. 4, 2014, p.2037-2064.

HWANG, T. Herdict: a distributed model for threats online. **Network Security**, [s.l], v. 2007, n. 8, ago. 2007, p. 15-18. Disponível em: <http://10.1016/S1353-4858(07)70074-0> Acesso em: 25 abr 2015.

I JUST doubled my pia VPN throughput that i am getting on my router by switching from UDP: 1194 to TCP:443. [s.l], 2014. Disponível em: <https://redd.it/1xkbca> Acesso em: 28 out 2015.

ICASA – INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA. **Home**. [s.l], 2017. Disponível em: <https://www.icasa.org.za> Acesso em: 30 jun 2017

IDEC - INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. [s.l], 2017. Disponível em: <http://www.idec.org.br/> Acesso em: 10 mar 2017.

IDEC: PLC 79 dá muito poder a Anatel e executivo e ignora o marco civil da Internet. [s.l], 2017. Disponível em: <http://www.telesintese.com.br/idec-critica-tramitacao-do-plc-79>. Acesso em: 14 abr 2017.

INTERNET LIVE STATS. **Internet Users**.[s. l], [2017a]. Disponível em: <http://www. internetlivestats. com/internet-users> Acesso em: 09 jun 2017

INTERNET LIVE STATS. **Total number of Websites**.[s. l], [2017b]. Disponível em: <http://www. internetlivestats. com/total-number-of-websites> Acesso em: 09 jun 2017

INTERNET SOCIETY. **Neutralidade da Rede**: um documento informativo sobre política pública da Internet Society. [s. l], 2015b. Disponível em: <https://www. internetsociety. org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030-PT-nb. pdf> Acesso em: 07 jun 2017

INTERNET SOCIETY.**Net Neutrality**. [s.l], 2015a. Disponível em: <http://www.internetsociety.org/net-neutrality?gclid=Cln0NGnzLICFGP0n AodZX8AXw> Acesso em: 01 mai 2015.

INTERNET WORLD STATS. **World Internet Usage and Population Statistics, March 31, 2017**. [s.l], 2017. Disponível em: <http://www.internetworldstats.com/stats.htm> Acesso em: 28 jun 2017

INTERNETNZ leads discussion on Net Neutrality in NZ. **Scoop Independent News**, [s.l], 2015. Disponível em: <http://www.scoop.co.nz/stories/BU1506/S00710/internetnz-leads-discussion-on-net-neutrality-in-nz.htm> Acesso em: 16 abr 2016.

ITU - International Telecommunication Union. **The ICT Development Index (IDI)**: conceptual framework and methodology. 2017. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2015/methodology.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society Report**: 2014. Switzerland: [s.n], 2014. Disponível em: <http://www.itu.int/en/ITU-

D/Statistics/Pages/publications/mis2014.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society Report**: 2016. Switzerland: [s.n], 2016. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2016.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society**: 2010. Switzerland: [s.n], 2010. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2010.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society**: 2012. Switzerland: [s.n], 2012. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2012.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society**: 2013. Switzerland: [s.n], 2013. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx> Acesso em: 22 mai 2017

ITU – International Telecommunication Union. **Measuring the Information Society**: the ICT development Index 2009.Switzerland: [s.n], 2009. Disponível em: <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2009.aspx> Acesso em: 22 mai 2017

ITU - INTERNATIONAL TELECOMMUNICATION UNION; UNESCO.The State of Broadband: broadband catalyzing sustainable development. [s. l]: BROADBAND COMISSION, 2016. Disponível em: <http://broadbandcommission. org/Documents/reports/bb-annualreport2016. pdf>Acesso em: 20 jun 2017

IX.BR. **Ponto de Intercambio de Internet**. [s.l], 2017. Disponível em: <http://ix.br/> Acesso em 02 jan 2017.

JOCH, A. Debating net neutrality. **Communications of the ACM**, [s.l], v. 52, n. 10, out. 2009, p. 14-15. Disponível em: <http://10.1145/1562764.1562773> Acesso em: 05 jan 2015.

JORDAN, S. Four questions that determine whether traffic management is reasonable. **International Symposium on Integrated Network Management**, [s.l], 2009a, p.137-140.

JORDAN, S. Some traffic management practices are unreasonable. **International Conference on Computer Communications and Networks**, [s.l], 2009b, p. 1-6.

JUKIC, Z. *et al*. Technical aspects of network neutrality. In: INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 11., 2011. **Anais…** Austria: [s.n], jun 15-17, 2011, p. 405 – 410.

KAKHKI , A. Molavi et al. Identifying Traffic Differentiation in Mobile Networks. In : INTERNET MEASUREMENT CONFERENCE. 2015. **Anais…** [s.l]: ACM, 2015, p. 239–251

KANUPARTHY, P.; DOVROLIS, C. DiffProbe: Detecting ISP Service Discrimination. In IEEE INFOCOM. 2010. **Anais…** [s.l: s.n], 2010.

KANUPARTHY, P.; DOVROLIS, C. ShaperProbe: End-to-end Detection of ISP Traffic Shaping Using Active Methods. In: SIGCOMM CONFERENCE ON INTERNET MEASUREMENT CONFERENCE. 2011. **Anais…** [s.l]: ACM. 2011.

KARR, T. **Free Press**: court win gives fcc the power to protect net neutrality: U.S. Court of Appeals confirms the FCC's authority to stop ISPs from stifling free expression and innovation online. [s.n], 2016. Disponível em: <https://www.freepress.net/press-release/107455/free-press-court-win-gives-fcc-power-protect-net-neutrality> Acesso em: 29 mai 2017.

KCC – KOREA COMMUNICATIONS COMMISSION. **Annual report 2011**. [s.l], 2012. Disponível em: <https://2013mirimstudent12.files.wordpress.com/2013/02/annual_report_2011.pdf > Acesso em: 02 mai 2015.

KENDRICK, J. **T-Mobile Germany Blocks iPhone Skype Over 3G and WiFi**. [s.l], 2009. Disponível em: <https://gigaom.com/2009/04/06/t-mobile-germany-blocks-iphone-skype-over-3g-too> Acesso em 25 mar 2015.

KINZINGER, A. **H.R. 2666 - No Rate Regulation of Broadband Internet Access Act.** [s.l], 2016a. Disponível em: <http://www.gop.gov/bill/h-r-2666-no-rate-regulation-of-broadband-internet-access-act/> Acesso em: 29 abr 2016.

KINZINGER, A. **Rep. Kinzinger's Bill, H.R. 2666, Passes the House.** Washington, 2016. Disponível em: <http://kinzinger.house.gov/news/documentsingle.aspx?DocumentID=399309> Acesso em: 29 abr 2016.

KLEINA, N. **Ministro confirma: limite de dados na banda larga fixa vai começar em 2017**. [s.l], 2017. Disponível em: <https://www.tecmundo.com.br/internet/113408-ministro-confirma-limite-dados-banda-larga-fixa-comecar-2017.htm?utm_source=tecmundo.com.br&utm_medium=home&utm_campaign=tv>. Acesso em: 08 abr 2017.

KRÄMER, J.; WIEWIORRA, L.; WEINHARDT, C. Net neutrality: a progress report. **Telecommunications Policy**, [s.l], n. 37, 2013, p. 794–813.

KREIBICH, C. *et al*. Netalyzr: illuminating the edge network. In: SIGCOMM CONFERENCE ON INTERNET MEASUREMENT. 10. 2010. **Anais…** [s.l]: ACM, 2010.

KROES, N. Net neutrality: the way forward. **SPEECH**, 2010. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-10-643_en.htm> Acesso em: 15 mai 2015.

KVALBEIN, A. *et al*. The Nornet Edge platform for mobile broadband measurements.

Computer Networks, [s.l], v. 61, 2014, p. 88–101.

LALANNE, F. *et al*. Adkintun Mobile: towards using personal and device context in assessing mobile QoS. In: INTERNATIONAL WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE, 2015. **Anais…** Dubrovnik, Croatia : [s.n], 24-28 ago. 2015, p. 49-54.

LARSON, N. *et al*. Investigating Excessive Delays in Mobile Broadband Networks. In: WORKSHOP ON ALL THINGS CELLULAR: OPERATIONS, APPLICATIONS AND HALLENGES, 5., 2015. **Anais…** [s.l: s.n], 2015. Disponível em: <http://dx.doi.org/10.1145/2785971.2785980>Acesso em: 21 out 2015.

LAYTON, R.; HORNEY, M. Innovation, Investment, and Competition in Broadband and the Impact on America's Digital Economy.**Mercatus Working Paper**, 2014. Disponível em: <https://www.mercatus.org/system/files/Layton-Competitionin-Broadband.pdf> Acesso em: 28mai. 2017

LEE, M. **S.2602 - Restoring Internet Freedom Act.** [s.l], 2016. Disponível em: <https://www.congress.gov/bill/114th-congress/senate-bill/2602/text> Acesso em: 29 abr 2016.

LEMLEY, M. A.; LESSIG, L. The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. UCLA Law Review, V. 48, 2001. Disponível em: <https://ssrn. com/abstract=247737 or http://dx. doi. org/10. 2139/ssrn. 247737>Acesso em: 19 jun 2017

LEMOS, R. **Internet brasileira precisa de marco regulatório civil**. [s.l], 2007. Disponível em: <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm> Acesso em: 21 jan 2016.

LESSIG, L. **The future of ideas:** the fate of the commons in a connected world. New York: Random House, 2001. 368p.

LETTER to FCC chairman Tom Wheeler. [s.l], 2014. Disponível em: <http://www.wyden.senate.gov/download/?id=26d1f814-1077-4cc2-bd85-026acd10c256&download=1> Acesso em: 19 ago 2015.

LING, F. Y. *et al*. Research on the Net neutrality: the Case of Comcast Blocking. In: INTERNATIONAL CONFERENCE ON ADVANCED COMPUTER THEORY AND ENGINEERING, 5., 2010. **Anais…** [s.l: s.n], 2010. p. 488-491.

LOMAS, N. **Verizon Accused Of Net Neutrality Foul By Zero-Rating Its Go90 Mobile Video Service**. [s.l], 2016. Disponível em: <http://techcrunch.com/2016/02/07/verizon-accused-of-net-neutrality-foul-by-zero-rating-its-go90-mobile-video-service/> Acesso em: 01 mai 2016.

LU, G. *et al*. POPI: A User-Level Tool for Inferring Router Packet Forwarding Priority**. IEEE/ACM Transactions on Networking**, [s.l], v. 18, n. 1, 2010.

MAHAJAN, R. *et al*. Uncovering Performance Differences Among Backbone ISPs with Netdiff. In: USENIX SYMPOSIUM ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION. 2008. **Anais…** [s.l: s.n]. 2008.

MANN, H. B.; WHITNEY, D. R. On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. **The Annals of Mathematical Statistics**, [s.l], v. 18, n. 1, 1947.

MARSDEN, C. T. Net Neutrality: the European debate. **Journal of Internet Law**, [s.l], v. 12, n. 2, ago. 2008, 11p.

MARTIN, J. C. D.; GLORIOSO, A. The Neubot project: A collaborative approach to measuring internet neutrality. In: IEEE INTERNATIONAL SYMPOSIUM ON TECHNOLOGY AND SOCIETY. 2008. **Anais…** [s.l: s.n]. 2008.

MEXICO. PODER EJECUTIVO. SECRETARIA DE COMUNICACIONES Y TRANSPORTES. Decreto por el que se expiden La Ley Federal de Telecomunicaciones y Radiodifusión, y La Leydel Sistema Público de Radiodifusióndel Estado Mexicano; y se reforman, adicionan y derogan diversas disposiciones em materia de telecomunicaciones y radiodifusión. **Diario Oficial**, [s.l], 2014. Disponível em: <http://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf> Acesso em: 17 jun 2015.

MIAC - MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS. **New Competition Promotion Program 2010**. Japão, 2006. Disponível em: <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/060928_1.pdf> Acesso em 03 jul 2015.

MIAC - MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS. **Report on Network Neutrality:** working group on Network Neutrality. Japão, 2007. Disponível em: <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf> Acesso em 27 mai 2015.

MIAC - MINISTRY OF INTERNAL AFFAIRS AND COMMUNICATIONS. Study Group Report: Report from Panel on Neutrality of Networks. **MIC Communications News**, Japão, v. 18, n. 23, mar. 2008. Disponível em: <http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol18/Vol18_23/Vol18_23.html> Acesso em: 18 jun 2015.

MICHAUT, F.; LEPAGE, F. Application-oriented network metrology: metrics and active measurement tools. **IEEE Communications Surveys Tutorials**, [s.l], v. 7, n. 2, 2005.

MINHA CONEXAO. **Velocímetro e teste da internet**. [s.l], 2017. Disponível em: <http://www.minhaconexao.com.br/>. Acesso em: 14 mar 2017.

MIORANDI *et al*. Measuring net neutrality in mobile Internet: towards a crowdsensing based citizen observatory. In: IEEE International Conference on Communications Workshops, 2013. **Anais..** [s.l]: ICC, p. 199–203.

MJC - MINISTÉRIO DA JUSTIÇA E CIDADANIA. **CADE**. [s.l], 2017. Disponível em: <http://www.justica.gov.br/Acesso/institucional/sumario/quemequem/autarquia-conselho-administrativo-de-defesa-economica-CADE> Acesso em: 03 jan 2017.

MPF - MINISTÉRIO PÚBLICO FEDERAL. [s.l], 2017. Disponível em: <http://www.mpf.mp.br/> Acesso em 02 jan 2017.

MUELLER, M. L.; ASGHARI, H. Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States. **Telecommunications Policy**, n. 36, 2012, p. 462-475.

NET neutrality debate: TRAI aims to resolve some issues by early 2016. **The Indian Express,** 2015b. Disponível em: <http://indianexpress.com/article/technology/tech-news-technology/trai-aims-to-resolve-some-net-neutrality-issues-by-early-2016/> Acesso em: 11 jan 2016.

NET neutrality monitor. [s.l], 2015a. Disponível em: <http://www.neumon.org> Acesso em 08 dez 2015.

NETWORK neutrality in New Zealand: public discussion document. [s.l], 2015. Disponível em: <https://internetnz.nz/sites/default/files/submissions/Network%20Neutrality%20Discussion%20Document%20-%20June%202015%20FINAL.pdf> Acesso em 22 abr 2016.

NETWORK neutrality: guidelines for Internet neutrality: version 1.0. fev. [s.l], 2009. Disponível em: <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Guidelines_for_network_neutrality_-_Norway.pdf>Acesso em 07 mai 2015.

NIC Chile research labs. [s.l], 2015. Disponível em: <http://www.niclabs.cl> Acesso em: 12 out 2015.

NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. [s.l], 2017. Disponível em: <http://nic.br/> Acesso em 02 jan 2017.

NKOM - NORWEGIAN COMMUNICATIONS AUTHORITY. **The Norwegian model**. [s.l], 2013. Disponível em: <http://eng.nkom.no/technical/internet/net-neutrality/the-norwegian-model>Acesso em: 07 mai 2015.

NNSQUAD. [s.l], 2015. Disponível em: <http://www.nnsquad.org/agent.html> Acesso em: 17 abr 2015.

NOVA ZELÂNDIA. MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT**. Regulating communications for the future**: review of the telecommunications act 2001. [s.l], 2015. Disponível em: <http://www.mbie.govt.nz/info-services/sectors-industries/technology-communications/communications/regulating-the-telecommunications-sector/review-of-the-telecommunications-act-2001/consultation-8-sept-2015/telecommunications-review-2015> Acesso em: 22 abr

2016.

NOVA ZELÂNDIA. MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT. **Submissions received**. [s.l, 2001]. Disponível em: <http://www.mbie.govt.nz/info-services/sectors-industries/technology-communications/communications/regulating-the-telecommunications-sector/review-of-the-telecommunications-act-2001/submissions-received/?searchterm=act%202001%2A> Acesso em: 23 abr 2016.

O'NEILL, R. **Internet NZ ignites net neutrality debate**: net neutrality is barely discussed in New Zealand, but market changes make a conversation necessary, says Internet NZ. [s.l], 2015. Disponível em: <http://www.zdnet.com/article/internet-nz-ignites-net-neutrality-debate> Acesso em 16 abr 2016.

O'RIELLY, M. **Shining the Spotlight**: how FCC rules impact consumers and industries. [s.l], 2016. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DOC-338600A1.pdf> Acesso em: 30 abr 2016.

OBSERVATÓRIO da Internet no Brasil. [s.l], 2016a. Disponível em: <http://observatoriodainternet.br>. Acesso em: 30 out 2016.

OBSERVATÓRIO do Marco Civil da Internet. [s.l], 2016b. Disponível em: <http://omci.org.br>. Acesso em: 30 out 2016.

OECD - ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Economic and Social Benefits of Internet Openness**.[s.l]: OECD, 2016. Disponível em: <http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En> Acesso em: 20 jun 2017

OECD – ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Communications Outlook 2013**. Paris: OECD Publishing, 2013. Disponível em: <http://dx.doi.org/10.1787/comms_outlook-2013-en> Acesso em: 22 mai 2017

OLMOS, A.; CASTRO, J. **Net Neutrality in the EU**: country factsheets. [s.l], 2013. Disponível em: <http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20-%20Country%20Factsheets%2020130905.pdf > Acesso em: 26 mai 2015.

ONLINE censorship in China.[s.l.], 2015.Disponível em: <https://en.greatfire.org/> Acesso em: 02 dez 2015.

OOKLA SPEEDTEST. [s.l], 2015. Disponível em: <https://www.ookla.com> Acesso em 10 dez 2015

PANORAMA setorial da Internet: os provedores de acesso à Internet no Brasil: como atuam e qual sua importância para o desenvolvimento da Internet brasileira. **Provimento de Acesso à Internet**, [s.l], n.2, 2016.

POWELL, M. K. **Preserving internet freedom**: guiding principles for the industry. Colorado, 2004. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf> Acesso em: 12 ago 2015.

PRESCOTT, R. **Minuta da regulamentação não avança em zero rating**. [s.l], 2016. Disponível em: <http://www.abranet.org.br/Noticias/Minuta-da-regulamentacao-nao-avanca-em-zero-rating-962.html#.Vsyk__krKUl> Acesso em: 23 fev 2016.

PROTESTE. [s.l], 2017. Disponível em: <https://www.proteste.org.br> Acesso em: 19 mar 2017.

PROTESTE. **55% dos testes de velocidade de Internet estão abaixo do contratado**. [s.l], 2015. Disponível em: <https://www.proteste.org.br/suas-contas/telefonia-fixa-e-movel/noticia/55-dos-testes-de-velocidade-de-internet-estao-abaixo-do-contratado> Acesso em: 19 mar 2017.

PROTESTE. **PROTESTE é contra a aplicação da franquia nos planos de acesso a banda larga**: há ação em andamento contra o bloqueio após fim da franquia do 3G. [s.l], 2016. Disponível em: <https://www.proteste.org.br/institucional/imprensa/press-release/2016/proteste-e-contra-a-aplicacao-da-franquia-nos-planos-de-acesso-a-banda-larga> Acesso em: 14 abr 2017.

PUBLIC KNOWLEDGE. **Sign the Petition**: protect Net Neutrality! [s.l], 2017. Disponível em: https://petitions.signforgood.com/ProtectNetNeutrality/?code=PK. Acesso em: 24 mai 2017.

QIU, T. *et al*. Packet Doppler: Network Monitoring Using Packet Shift Detection. In: ACM CoNEXT Conference. **Anais…** [s.l]: ACM. 2008.

RAVAIOLI, R.; BARAKAT, C.; URVOY-KELLER, G. Chkdiff: Checking Traffic Differentiation at Internet Access. In: ACM Conference on CoNEXT Student Workshop. 2012. **Anais…** [s.l]: ACM. 2012

RAVAIOLI, R.; URVOY-KELLER, G.; BARAKAT, C. Towards a General Solution for Detecting Traffic Differentiation at the Internet Access. In: Teletraffic Congress (ITC). 2015. **Anais…** [s.l: s.n]. 2015.

REGISTRO. [s.l], 2017. Disponível em: <http://www.registro.br/> Acesso em 02 jan 2017.

REGULATION (EC) No 1211/2009 of the European Parliament and of the Council. **Official Journal of the European Union**, 2009. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:EN:PDF> Acesso em: 21 mar 2016.

REIS, C. *et al*. Detecting in-flight page changes with web tripwires**.** In: USENIX SYMPOSIUM ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION, 5., 2008.

Proceedings.. Berkeley, CA, USA: [s.n], 31-44 p.

RESPECT my net: name and shame operators restricting access to the Internet. [s.l], 2015. Disponível em: <http://respectmynet.eu/> Acesso em 27 out 2015.

REVISION history of "Bad ISPs". [s.l], 2005. Disponível em: <https://wiki.vuze.com/mediawiki/index.php?title=Bad_ISPs&dir=prev&action=history> Acesso em: 21 set 2015.

RISLEY, J. **Report**: Comcast data caps result in more than 13,000 FCC complaints. [s.l], 2015. Disponível em: <http://www.geekwire.com/2015/report-comcast-data-caps-result-in-more-than-13000-fcc-complaints-including-questions-about-accuracy/> Acesso em: 01 mai 2016.

RNP - REDE NACIONAL DE ENSINO E PESQUISA. [s.l], 2017. Disponível em: <https://www.rnp.br/> Acesso em 26 jan 2017.

ROY, P. K. India's fight for net neutrality. **BBC News**, [s.l], 2015. Disponível em: <http://www.bbc.com/news/world-asia-india-32313704>Acesso em: 11 jan 2016.

S. 2602 (114th): Restoring Internet Freedom Act. [s.l], 2017. Disponível em: <https://www.govtrack.us/congress/bills/114/s2602>. Acesso em: 21 abr 2017.

SADAUSKAS, A. **Australia needs to have a conversation about Net(work) Neutrality**: NBN chairman. [s.l], 2015. Disponível em: <http://www.itnews.com.au/news/australia-needs-to-have-a-conversation-about-net-neutrality-says-nbn-chairman-411946> Acesso em: 12 abr 2016.

SAMKNOWS. [s.l], 2015. Disponível em: <https://www.samknows.com> Acesso em 16 fev 2017

SÁNCHEZ, M. A. *et al*. E. Dasu - ISP Characterization from the Edge: a BitTorrent Implementation. **SIGCOMM Computer Communication Review**, [s.l], v. 41, n. 4, 2011.

SAVE THE INTERNET. **Stop the Trump administration's attack on Net(work) Neutrality**. [s.l], 2017. Disponível em: <https://www.savetheinternet.com/sti-home> Acesso em: 24 mai 2017.

SBC - SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. **Grandes Desafios da Pesquisa em Computação no Brasil 2006 – 2016**: Relatório sobre o Seminário realizado em 8 e 9 de maio de 2006. [s.l], 2016. 26 p. Disponível em: http://www.sbc.org.br/documentos-da-sbc/send/141-grandes-desafios/798-grandesdesafios-portugues. Acesso em: 14 abr 2017.

SCOTT, M. Tim Berners-Lee, Web Creator, Defends Net Neutrality. **The New York Times**. [s.l], 2014. Disponível em: <Disponível em : http://bits.blogs.nytimes.com/2014/10/08/tim-berners-lee-web-creator-defends-net-neutrality/?_r=0> Acesso em: 01 mai 2015.

SENACON - SECRETARIA NACIONAL DO CONSUMIDOR. [s.l], 2017. Disponível em: <https://www.consumidor.gov.br/> Acesso em 25 mar 2017

SERRAL-GRACIA, R. *et al* . An efficient and lightweight method for Service Level Agreement assessment. **Computer Networks**, [s.l], v. 54, n. 17, 2010.

SERRAL-GRACIA, R. *et al* . Towards an Efficient Service Level Agreement Assessment. In: IEEE INFOCOM. **Anais…** [s.l; s.n]. 2009.

SFAKIANAKIS, A.; ATHANASOPOULOS, E.; IOANNIDIS, S. **CensMon**: a web censorship monitor. [s.l], 2011. Disponível em: <https://www.usenix.org/legacy/events/foci11/tech/final_files/Sfakianakis.pdf> Acesso em 25 mar 2015

SHANKESI, R. **Friendsourcing to detect network manipulation**. 94 f. Dissertação, University of Illinois, Urbana, 2013. Disponível em: <https://www.ideals.illinois.edu/bitstream/handle/2142/45321/Ravinder_Shankesi.pdf?sequence=1> Acesso em: 02 out 2015.

SILVA, S.; BIONDI, A. **Caminhos para a universalização da Internet banda larga**: experiências internacionais e desafios brasileiros. São Paulo: Intervozes, 2012. Disponível em: <http://www. intervozes. org.br/arquivos/interliv008cpunibl> Acesso em: 24 abr 2017

SIMET - SISTEMA DE MEDIÇÃO DE TRÁFEGO INTERNET**.** [s.l], 2017. Disponível em: <http://simet.nic.br/>. Acesso em: 14 mar 2017.

SIMET BOX. [s.l], 2017. Disponível em: <http://simet.nic.br/simetbox.html>. Acesso em: 14 mar 2017.

SIMET MOBILE. [s.l], 2017. Disponível em: <http://simet.nic.br/sobresimetmobile.html> Acesso em: 15 mar 2017.

SOMMERS, J. *et al*. Accurate and Efficient SLA Compliance Monitoring. **SIGCOMM Computer Communication Review**, [s.l], v. 37, n. 4, 2007.

SOMMERS, J. *et al*. Multiobjective Monitoring for SLA Compliance. **IEEE/ACM Transactions on Networking**, [s.l], v. 18, n. 2, 2010.

SØRENSEN, F. **Net neutrality and charging models**. [s.l], [2014b]. Disponível em: <http://eng.nkom.no/topical-issues/news/net-neutrality-and-charging-models> Acesso em 01 mai 2016.

SØRENSEN, F. **The net neutrality service model explained**. [s.l], [2014a]. Disponível em: <http://eng.no/technical/internet/net-neutrality/the-norwegian-model/_attachment/12631?_ts=1452775f759> Acesso em: 07 mai 2015.

SPEEDCHECKER. [s.l], 2015. Disponível em: <http://www.broadbandspeedchecker.co.uk> Acesso em: 14 dez 2015.

SPEEDTESTE. [s.l], 2017. Disponível em: <http://www.speedteste.com.br/> Acesso em 06 mar 2017.

SQUEO, A. M. Help**ing Netflix Members Get More from Their Mobile Data Plans**. [s.l], 2016. Disponível em: <https://media.netflix.com/en/company-blog/helping-netflix-members-get-more-from-their-mobile-data-plans> Acesso em: 30 abr 2016.

SUBTEL - SUBSECRETARÍA DE TELECOMUNICACIONES. **Ley de Neutralidad y Redes Sociales Gratis.** [s.l], 2014. Disponível em <http://www.subtel.gob.cl/ley-de-neutralidad-y-redes-sociales-gratis/> Acesso em: 24 abr 2016.

SUBTEL - SUBSECRETARÍA DE TELECOMUNICACIONES. **SUBTEL instruye y exige a empresas de internet mayor transparencia en planes de banda ancha por Ley de Neutralidad de Red**. [s.l], 2011. Disponível em: <http://www.subtel.gob.cl/subtel-instruye-y-exige-a-empresas-de-internet-mayor-transparencia-en-planes-de-banda-ancha-por-ley-de-neutralidad-de-red/> Acesso em: 24 abr 2016.

SWITZERLAND network testing tool. [s.l], 2015. Disponível em: <https://www.eff.org/pages/switzerland-network-testing-tool> Acesso em: 18 mar 2015.

TA, X.; MAO, G. Online End-to-End Quality of Service Monitoring for Service Level Agreement Verification. **IEEE International Conference on Networks**, [s.l], v. 2, 2006.

TARIQ, M. B. *et al*. Detecting Network Neutrality Violations with Causal Inference. In: International Conference on Emerging Networking Experiments and Technologies (CoNEXT). 2009. **Anais…** [s.l]: ACM, 2009.

TELEBRASIL - ASSOCIAÇÃO BRASILEIRA DE TELECOMUNICAÇÕES. [s.l], 2017. Disponível em: <http://www.telebrasil.org.br> Acesso em 30 jan 2017.

TELL TRAI that we need net neutrality, once again. [s.l], 2015. Disponível em: <https://www.savetheinternet.in/> Acesso em: 11 jan 2016

TELUS cuts subscriber access to pro-union website. [s.l], 2005. Disponível em: <http://www.cbc.ca/news/canada/telus-cuts-subscriber-access-to-pro-union-website-1.531166> Acesso em: 04 mar 2016.

TESTE COPEL. **Teste de velocidade de conexão de internet da Copel**. Curitiba, 2017. Disponível em: <http://testecopel.org/> Acesso em: 18 mar 2017

TESTMY.NET. [s.l], 2015. Disponível em: <http://testmy.net> Acesso em 14 dez 2015.

THE FIGHT for net neutrality in europe is not over. [s.l], 2015. Disponível em: <https://savetheinternet.eu> Acesso em: 23 dez 2015.

THE STATE of Broadband 2014: broadband for all. [s. l], [2014]. Disponível em: <http://www. broadbandcommission. org/Documents/publications/bb-State-of-Broadband-2014-flyer. pdf>Acesso em: 19 jun 2017

TOPOLSKI, R. **Comcast is using Sandvine to manage P2P Connections**. [s.l], 2007. Disponível em: <http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections. Acesso em 27 mar 2015> Acesso em : 27 mar 2015.

TRAI - TELECOM REGULATORY AUTHORITY OF INDIA. **Consultation Paper On Regulatory Framework for Over-the-top (OTT) services.** Nova Deli, 2015a. Disponível em: <http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/ OTT-CP-27032015.pdf>. Acesso em: 27 mai 2015.

TRAI - TELECOM REGULATORY AUTHORITY OF INDIA. **Consultation Paper on Differential Pricing for Data Services.** Nova Deli, 2015b. Disponível em: <http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/CP-Differential-Pricing-09122015.pdf> Acesso em: 17 fev 2016.

TRAI - TELECOM REGULATORY AUTHORITY OF INDIA. **Prohibition of discriminatory tariffs for data services regulations**. Nova Deli, 2016. Disponível em: <http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf>Acesso em: 16 fev 2016.

TRESTIAN, I.; POTHARAJU, R.; KUZMANOVIC, A**.** **WindRider**: a mobile network neutrality monitoring system. [s.l], [2017]. Disponível em: <http://networks.cs.northwestern.edu/mobile-neutrality> Acesso em: 16 out 2017

UN - THE UNITED NATIONS. **Internet governance must ensure access for everyone – UN expert**. [s. l], 2012. Disponível em: <http://www. un. org/apps/news/story. asp?NewsID=42039#. WWd_RdQrKHs> Acesso em: 20 jun 2017

UNITED STATES OF AMERICA. **H.R.5353**: Internet Freedom Preservation Act of 2008. [s.l], 2008. Disponível em: <https://www.congress.gov/110/bills/hr5353/BILLS-110hr5353ih.pdf> Acesso em: 13 ago 2015.

UNITED STATES OF AMERICA. Mo**tion of the FCC to dismiss case nº. 15-1063 and 15-1078**. [s.l], 2015. Disponível em: <https://apps.fcc.gov/edocs_public/attachmatch/DOC-333492A1.pdf> Acesso em: 29 abr 2016.

VAN SCHEWICK, B. **T-Mobile's Binge On Violates Key Net Neutrality Principles**. [s.l], 2016. Disponível em: <https://prodnet.www.neca.org/publicationsdocs/wwpdf/2216she.pdf>. Acesso em 24 abr 2016.

VAN SCHEWICK, B.; FARBER, D. Network neutrality nuances: a discussion of divergent paths to unrestricted access of content and applications via the Internet. **Communications of the ACM**, [s.l], v. 52, n. 2, fev. 2009, p. 31-37. Disponivel em: <ttp://dx.doi.org/10.1145/1461928.1461942> Acesso em: 22 out 2015.

VAN SCHEWICK, B. Network neutrality: what a non-discrimination rule should look like. In: RESEARCH CONFERENCE ON COMMUNICATION, INFORMATION AND

INTERNET POLICY, 38. ,2010, Arlington. **Anais…** Stanford: Stanford Law and Economics Olin Working Paper, n. 402, 2010. Disponível em: <http://dx. doi. org/10. 2139/ssrn. 1684677> Acesso em: 24 abr 2017

VISHWANATH, K. V.; VAHDAT, A. Swing: Realistic and Responsive Network Traffic Generation. **IEEE/ACM Transactions on Networking**, [s.l], v. 17, n. 3, 2009.

W3C BRASIL. [s.l], 2017. Disponível em: <http://www.w3c.br>. Acesso em 02 jan 2017.

WEAVER, N.; SOMMER, R.; PAXSON, V. Detecting Forged TCP Reset Packets. In: NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. 2009. **Anais…** [s.l: s.n]. 2009.

WEBER, M. *et al*. Can HAKOMetar be Used to Increase Transparency in the Context of Network Neutrality? In: INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS, 12., 2013. **Anais..** Croatia: [s.n], jun 26-28, 2013, p. 309 – 316.

WEINSBERG, U.; SOULE, A.; MASSOULIE, L. Inferring traffic shaping and policy parameters using end host measurements. In: IEEE INFOCOM. 2011. **Anais…** [s.l: s.n], 2011.

WEITZNER, D. J. Net Neutrality… Seriously this Time. **Internet Computing**, [s.l], v. 12, n. 3, mai.-jun. 2008. p.86-89.

WHITEBOX. [s.l], 2015. Disponível em: <https://www.samknows.com> Acesso em: 16 dez 2015.

WORLD BANK. **Investment in telecoms with private participation (current US$)**. 2017a. Disponível em: <http://data.worldbank.org/indicator/IE.PPI.TELE.CD> Acesso em: 22 mai 2017

WORLD BANK. **Population, total**. 2017b. Disponível em: <http://data.worldbank.org/indicator/NY.GDP.MKTP.KN> Acesso em: 22 mai 2017

WORLD WIDE WEB FOUNDATION. **Net Neutrality in Europe**: a statement from Sir Tim Berners-Lee. [s.l], 2015. Disponível em: <http://webfoundation.org/2015/10/net-neutrality-in-europe-a-statement-from-sir-tim-berners-lee> Acesso em 21 dez 2015.

WU, T. **A Proposal for Network Neutrality**.[s.l], 2002. Disponível em: <http://www.timwu.org/OriginalNNProposal.pdf> Acesso em: 25 set 2015.

WU, T. Network Neutrality, Broadband Discrimination. **Journal of Telecommunications and High Technology Law**, [s.l], v. 2, 2003.p.141 -179.

WU, T.; LESSIG, L. **Letter to FCC**, [s.l], 2003.Disponível em: <http://www.savetheinternet.com/sites/default/files/resources/wu_lessig_fcc.pdf>Acesso em: 16 jan 2015.

YOO, C. Beyond Network Neutrality. **Harvard Journal of Law & Technology**, v. 19, n. 1, 2005.Disponível em: <http://jolt. law. harvard.

edu/articles/pdf/v19/19HarvJLTech001. pdf> Acesso em: 19 jun 2017

ZAMBIA, a country under Deep Packet Inspection. [s.l], 2013. Disponível em: <https://ooni.torproject.org/post/zambia> Acesso em: 2015/09/17.

ZHANG, Y.; MAO, Z. M.; ZHANG, M. Detecting traffic differentiation in backbone ISPs with NetPolice. In: SIGCOMM. 9. 2009. **Anais…** Chicago: ACM, 2009. Disponível em: <10.1145/1644893.1644905>. Acesso em: 25 mar 2015.

ZHANG, Y; MAO, Z.M; ZHANG, M. Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs. [s.l], 2008. Disponível em: <http://msr-waypoint.com/en-us/um/people/mzh/papers/nvlens.pdf>. Acesso em: 25 mar 2015.

ZHANG, Z.; MARA, O.; ARGYRAKI, K. Network neutrality inference**.** In: SIGCOMM. 14. 2014. **Anais..** Chicago: [s.n], 2014. Disponível em: <http://infoscience.epfl.ch/record/186414/files/neutrality_inference.pdf>. Acesso em: 25 jan. 2015.